



INSTALL GUIDE

FortiWiFi-60A /AM
FortiOS 3.0 MR4

FORTINET™

www.fortinet.com

FortiWiFi-60A/AM Install Guide
FortiOS 3.0 MR4
15 February 2007
01-30004-0283-20070215

© Copyright 2006 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance

FCC Class A Part 15 CSA/CUS



Caution: If you install a battery that is not the correct type, it could explode. Dispose of used batteries according to local regulations.

Contents

| | |
|-------------------------------------------------------------------|-----------|
| Contents | 3 |
| Introduction | 7 |
| About the FortiWiFi unit | 7 |
| FortiWiFi-60A/AM | 7 |
| Register your FortiWiFi unit..... | 8 |
| Fortinet Family Products | 8 |
| FortiGuard Subscription Services | 8 |
| FortiClient..... | 8 |
| FortiMail | 9 |
| FortiAnalyzer | 9 |
| FortiReporter | 9 |
| FortiBridge..... | 9 |
| FortiManager..... | 9 |
| About this document | 10 |
| Document conventions..... | 10 |
| Typographic conventions..... | 11 |
| Fortinet documentation | 12 |
| Fortinet Knowledge Center | 13 |
| Comments on Fortinet technical documentation | 13 |
| Customer service and technical support | 13 |
| Installing the FortiWiFi unit | 15 |
| Package Contents | 15 |
| FortiWiFi-60A/AM | 15 |
| Mounting | 16 |
| Powering on the FortiWiFi unit | 16 |
| Powering off the FortiWiFi unit | 17 |
| Connecting to the FortiWiFi unit | 17 |
| Web-based manager..... | 17 |
| Command line interface | 17 |
| Connecting to the web-based manager | 18 |
| System Dashboard | 19 |
| Command line interface | 19 |
| Connecting to the CLI | 19 |
| Quick installation using factory defaults | 20 |
| Factory defaults | 23 |
| Factory default DHCP server configuration | 24 |
| Factory default NAT/Route mode network configuration | 24 |

| | |
|---------------------------------------------------------------------|-----------|
| Factory default Transparent mode network configuration..... | 25 |
| Factory default firewall configuration | 25 |
| Factory default protection profiles | 26 |
| Restoring the default settings..... | 27 |
| Restoring the default settings using the web-based manager | 27 |
| Restoring the default settings using the CLI | 27 |
| Configuring the FortiWiFi..... | 29 |
| Planning the FortiWiFi configuration | 29 |
| NAT/Route mode | 29 |
| NAT/Route mode with multiple external network connections | 30 |
| Transparent mode..... | 31 |
| NAT/Route mode installation | 32 |
| Preparing to configure the FortiWiFi unit in NAT/Route mode | 32 |
| DHCP or PPPoE configuration | 33 |
| Using the web-based manager | 33 |
| Configuring basic settings | 34 |
| Adding a default route | 35 |
| Verifying the web-based manager configuration | 35 |
| Verify the connection | 35 |
| Using the command line interface..... | 35 |
| Configuring the FortiWiFi unit to operate in NAT/Route mode | 35 |
| Adding a default route | 37 |
| Verify the connection | 38 |
| Connecting the FortiWiFi unit to the network(s)..... | 38 |
| Configuring the networks | 39 |
| Transparent mode installation | 40 |
| Preparing to configure Transparent mode | 40 |
| Using the web-based manager | 40 |
| Using the Command line interface..... | 41 |
| Connecting the FortiWiFi unit to your network | 42 |
| Verify the connection | 42 |
| Next steps | 43 |
| Set the date and time | 43 |
| Updating antivirus and IPS signatures | 44 |
| Updating antivirus and IPS signatures from the web-based manager .. | 44 |
| Updating the IPS signatures from the CLI | 45 |
| Scheduling antivirus and IPS updates..... | 45 |
| Adding an override server | 46 |
| Configuring the modem interface | 49 |
| Selecting a modem mode | 50 |
| Redundant mode configuration | 50 |
| Stand alone mode configuration | 50 |

| | |
|----------------------------------------------------------------------------|----|
| Configuring modem settings | 52 |
| Connecting and disconnecting the modem in Stand alone mode | 53 |
| Configuring the modem using the CLI | 54 |
| Adding a Ping Server | 56 |
| Dead gateway detection | 56 |
| Adding firewall policies for modem connections | 56 |
| Using a wireless network | 57 |
| Setting up a wireless network | 57 |
| Positioning an Access Point..... | 58 |
| Radio Frequency interface | 58 |
| Using multiple access points..... | 58 |
| Wireless Security | 59 |
| Wireless Equivalent Privacy (WEP) | 59 |
| Wi-Fi Protected Access (WPA) | 60 |
| Additional security measures | 60 |
| MAC address filtering | 60 |
| Service Set Identifier | 61 |
| FortiWiFi operation modes | 61 |
| Access Point mode | 61 |
| Client mode | 62 |
| Changing the operating mode | 62 |
| Setting up the FortiWiFi unit as an Access Point | 62 |
| Set the DHCP settings | 63 |
| Set the security options..... | 63 |
| Configure the firewall policies | 64 |
| FortiWiFi Firmware | 65 |
| Upgrading to a new firmware version | 65 |
| Upgrading the firmware using the web-based manager | 65 |
| Upgrading the firmware using the CLI | 66 |
| Reverting to a previous firmware version | 67 |
| Reverting to a previous firmware version using the web-based manager .. | 67 |
| Reverting to a previous firmware version using the CLI | 68 |
| Installing firmware images from a system reboot using the CLI | 70 |
| Restoring the previous configuration | 72 |
| The FortiUSB key | 72 |
| Backup and Restore from the FortiUSB key | 73 |
| Using the USB Auto-Install feature | 74 |
| Additional CLI Commands for the FortiUSB key | 75 |
| Testing a new firmware image before installing it | 75 |
| Index | 79 |

Introduction

Welcome and thank you for selecting Fortinet products for your real-time network protection.

The FortiGate™ Unified Threat Management System improves network security, reduces network misuse and abuse, and helps you use communications resources more efficiently without compromising the performance of your network. FortiGate Unified Threat Management Systems are ICSA-certified for firewall, IPSec, and antivirus services.

The FortiGate Unified Threat Management System is a dedicated, easily managed security device that delivers a full suite of capabilities, which include:

- application-level services such as virus protection and content filtering
- network-level services such as firewall, intrusion detection, VPN and traffic shaping

The FortiGate Unified Threat Management System uses Fortinet's Dynamic Threat Prevention System (DTPS™) technology, which leverages breakthroughs in chip design, networking, security and content analysis. The unique ASIC-based architecture analyzes content and behavior in real-time, enabling key applications to be deployed right at the network edge where they are most effective at protecting your networks.

About the FortiWiFi unit

The FortiWiFi-60A and FortiWiFi-60AM appliances are designed for small businesses (including telecommuters), to deliver the same enterprise-class network-based antivirus, content filtering, firewall, VPN, and network-based intrusion detection/prevention featured in all FortiGate units. The FortiWiFi-60A and FortiWiFi-60AM also feature High Availability (HA) support.

FortiWiFi-60A/AM

The FortiWiFi-60A (shown at right) and FortiWiFi-60AM provides a secure, wireless LAN solution for wireless connections. It combines mobility and flexibility with FortiWiFi Antivirus Firewall features, and can be upgraded to future radio technologies. The FortiWiFi-60A/AM unit supports wireless 802.11 a/b/g standards. The FortiWiFi-60AM unit features an internal modem that can also be used as either a backup or a stand alone connection to the Internet, while the FortiWiFi-60A supports an external modem connection via the USB port for the same purposes. The FortiWiFi-60A/AM serves as the connection point between wireless and wired networks or the center-point of a stand alone wireless network.



Register your FortiWiFi unit

Register your FortiWiFi unit by visiting <http://support.fortinet.com> and select Product Registration.

To register, enter your contact information and the serial numbers of the FortiWiFi units that you or your organization have purchased. You can register multiple FortiWiFi units in a single session without re-entering your contact information.

By registering your FortiWiFi unit, you will receive updates to threat detection and prevention databases (Antivirus, Intrusion Detection, etc.) and will also ensure your access to technical support.

Fortinet Family Products

Fortinet offers a family of products that includes both software and hardware appliances, for a complete network security solution including mail, logging, reporting, network management, and security along with FortiGate Unified Threat Management Systems. For more information on the Fortinet product family, go to www.fortinet.com/products.

FortiGuard Subscription Services

FortiGuard Subscription Services are security services created, updated and managed by a global team of Fortinet security professionals. They ensure the latest attacks are detected and blocked before harming your corporate resources or infecting your end-user computing devices. These services are created with the latest security technology and designed to operate with the lowest possible operational costs.

FortiGuard Subscription Services includes:

- FortiGuard Antivirus Service
- FortiGuard Intrusion Prevention subscription services (IPS)
- FortiGuard Web Filtering
- FortiGuard Antispam Service
- FortiGuard Premier Service

An online virus scanner and virus encyclopedia is also available for your reference.

FortiClient

FortiClient™ Host Security software provides a secure computing environment for both desktop and laptop users running the most popular Microsoft Windows operating systems. FortiClient offers many features including:

- creating VPN connections to remote networks
- configuring real-time protection against viruses
- guarding against modification of the Windows registry
- virus scanning

FortiClient also offers a silent installation feature, enabling an administrator to efficiently distribute FortiClient to several users' computers with preconfigured settings.

FortiMail

FortiMail™ Secure Messaging Platform provides powerful, flexible heuristic scanning and reporting capabilities to incoming and outgoing email traffic. The FortiMail unit has reliable, high performance features for detecting and blocking malicious attachments such as Distributed Checksum Clearinghouse (DCC) scanning and Bayesian scanning. Built on Fortinet's award winning FortiOS and FortiASIC technology, FortiMail antivirus technology extends full content inspection capabilities to detect the most advanced email threats.

FortiAnalyzer

FortiAnalyzer™ provides network administrators with the information they need to enable the best protection and security for their networks against attacks and vulnerabilities. The FortiAnalyzer unit features include:

- collects logs from FortiGate devices and syslog devices
- creates hundreds of reports using collected log data
- scans and reports vulnerabilities
- stores files quarantined from a FortiGate unit

The FortiAnalyzer unit can also be configured as a network analyzer to capture real-time traffic on areas of your network where firewalls are not employed. You can also use the unit as a storage device where users can access and share files, including the reports and logs that are saved on the FortiAnalyzer hard disk.

FortiReporter

FortiReporter™ Security Analyzer software generates easy-to-understand reports and can collect logs from any FortiGate unit, as well as over 30 network and security devices from third-party vendors. FortiReporter reveals network abuse, manages bandwidth requirements, monitors web usage, and ensures employees are using the office network appropriately. FortiReporter allows IT administrators to identify and respond to attacks, including identifying ways to proactively secure their networks before security threats arise.

FortiBridge

FortiBridge™ products are designed to provide enterprise organizations with continuous network traffic flow in the event of a power outage or a FortiGate system failure. The FortiBridge unit bypasses the FortiGate unit to make sure that the network can continue processing traffic. FortiBridge products are easy to use and deploy, and you can customize the actions a FortiBridge unit takes when a power failure or a FortiGate system failure occurs.

FortiManager

The FortiManager™ system is designed to meet the needs of large enterprises (including managed security service providers) responsible for establishing and maintaining security policies across many dispersed FortiGate installations. With this system, you can configure multiple FortiGate devices and monitor their status. You can also view real-time and historical logs for the FortiGate devices, including updating firmware images of managed FortiGate devices. The FortiManager System emphasizes ease of use, including easy integration with third party systems.

About this document

This document explains how to install and configure your FortiWiFi unit onto your network. This document also includes how to install and upgrade new firmware versions on your FortiWiFi unit.

This document contains the following chapters:

- [Installing the FortiWiFi unit](#) – Describes setting up, and powering on a FortiWiFi unit.
- [Factory defaults](#) – Provides the factory default settings for the FortiWiFi unit.
- [Configuring the FortiWiFi](#) – Provides an overview of the operating modes of the FortiGate unit and how to integrate the FortiWiFi unit into your network.
- [Configuring the modem interface](#) – Describes how to configure and use a modem with the FortiWiFi-60A/AM.
- [Using a wireless network](#) – Outlines the considerations for wireless networking and steps you can take to make your wireless network as efficient as possible.
- [FortiWiFi Firmware](#) – Describes how to install, update, restore and test the firmware for the FortiWiFi device.

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:



Note: Highlights useful additional information.



Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Typographic conventions

FortiWiFi documentation uses the following typographical conventions:

| Convention | Example |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Keyboard input | In the Gateway Name field, type a name for the remote VPN peer or client (for example, <code>Central_Office_1</code>). |
| Code examples | <pre>config sys global set ips-open enable end</pre> |
| CLI command syntax | <pre>config firewall policy edit id_integer set http_retry_count <retry_integer> set natip <address_ipv4mask> end</pre> |
| Document names | <i>FortiGate Administration Guide</i> |
| Menu commands | Go to VPN > IPSEC > Phase 1 and select Create New. |
| Program output | Welcome! |
| Variables | <address_ipv4> |

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

The following [FortiGate product documentation](#) is available:

- *FortiGate QuickStart Guide*
Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Install Guide*
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference*
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*
Available exclusively from the [Fortinet Knowledge Center](#), the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*
Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.
- *FortiGate SSL VPN User Guide*
Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*
Explains how to configure a PPTP VPN using the web-based manager.

- *FortiGate Certificate Management User Guide*
Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*
Describes how to configure VLANs and VDOMS in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.

Installing the FortiWiFi unit

This section provides information on installing and setting up the FortiWiFi unit on your network. This section includes the following topics:

- [Package Contents](#)
- [Mounting](#)
- [Powering on the FortiWiFi unit](#)
- [Connecting to the FortiWiFi unit](#)

Package Contents

Review the contents of your FortiWiFi package to ensure all components were included.

FortiWiFi-60A/AM

The FortiWiFi package contains the following items:

- FortiWiFi-60A or FortiWiFi-60AM Unified Threat Management System
- one orange crossover Ethernet cable (Fortinet part number CC300248)
- one gray straight-through Ethernet cable (Fortinet part number CC300249)
- one RJ-45 to DB-9 serial cable (Fortinet part number CC300247)
- one power cable and one AC adapter
- FortiWiFi-60A/AM QuickStart Guide
- two mounting brackets and screws
- Fortinet Documentation CD

Figure 1: FortiWiFi-60A/AM package contents

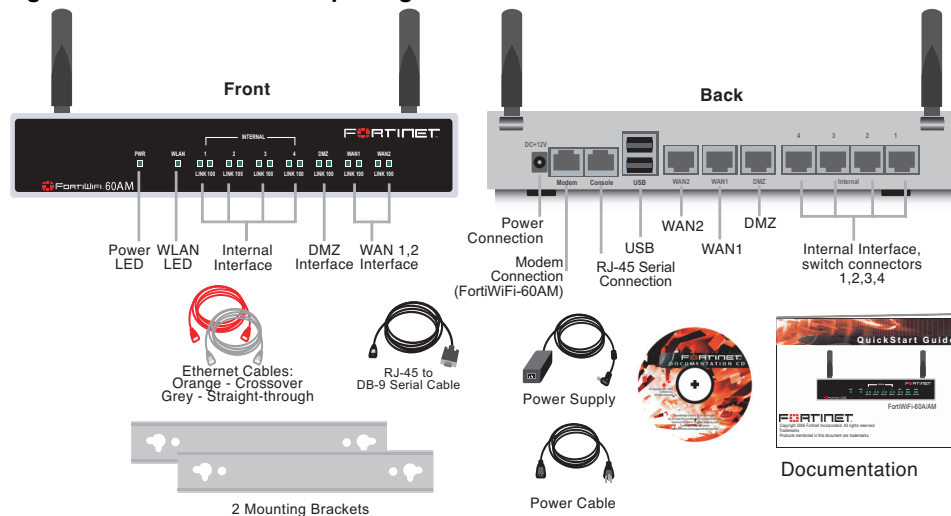


Table 1: Technical Specifications

| | |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Dimensions | 8.63 x 6.13 x 1.38 in. (21.9 x 15.6 x 3.5 cm) |
| Weight | 1.5 lb. (0.68 kg) |
| Power Requirements | DC input voltage: 12V DC input current: 3A |
| Wireless Connectivity | Antenna type: Dual external fixed antenna Antenna range: 802.11 a/b/g:2.4 - 5GHz Antenna Gain: 5dBi |
| Environmental Specifications | Operating temperature: 32 to 104 F (0 to 40 C) Storage temperature: -13 to 158 F (-25 to 70 C) Humidity: 5 to 95% non-condensing |

Mounting

Install the FortiWiFi unit on any stable, flat surface. Make sure the unit has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Powering on the FortiWiFi unit

The FortiWiFi unit does not have an on/off switch.

To power on the FortiWiFi unit

- 1 Connect the AC adapter to the power connection at the back of the FortiWiFi unit.
- 2 Connect the AC adapter to the power cable.
- 3 Connect the power cable to a power outlet.

The FortiWiFi unit starts and the Power and Status LEDs light up. The Status LEDs flash while the FortiWiFi unit starts up, and remain lit when the system is running.

Table 2: LED indicators

| LED | State | Description |
|-----------------------------------------------|----------------|--------------------------------------------------------------------|
| Power | Green | The FortiWiFi unit is powered on. |
| | Off | The FortiWiFi unit is powered off. |
| WLAN | Green | Traffic on WLAN link. |
| Link (Internal, DMZ, WAN1, WAN2) | Green | The correct cable is in use and the connected equipment has power. |
| | Flashing Green | Network activity at this interface. |
| | Off | No link established. |
| 100 (Internal, DMZ, WAN1, WAN2) | Green | The interface is connected at 100 Mbps. |

Powering off the FortiWiFi unit

Always shut down the FortiWiFi operating system properly before turning off the power switch to avoid potential hardware problems.

To power off the FortiWiFi unit

- 1 From the web-based manager, go to **System > Status**.
- 2 In the Unit Operation display, select Shutdown.
or from the CLI, enter:

```
execute shutdown
```
- 3 Disconnect the power supply.

Connecting to the FortiWiFi unit

There are two methods of connecting and configuring the basic FortiWiFi settings:

- the web-based manager
- the command line interface (CLI)

Web-based manager

You can configure and manage the FortiWiFi unit using HTTP or a secure HTTPS connection from any computer running Microsoft Internet Explorer 6.0 or recent browser. The web-based manager supports multiple languages.

You can use the web-based manager to configure most FortiWiFi settings, and monitor the status of the FortiWiFi unit.

Command line interface

You can access the FortiWiFi command line interface (CLI) by connecting a management computer serial port to the FortiWiFi serial console connector. You can also use Telnet or a secure SSH connection to connect to the CLI from any network that is connected to the FortiWiFi unit, including the Internet.

Connecting to the web-based manager

Use the following procedure to connect to the web-based manager for the first time. Configuration changes made with the web-based manager are effective immediately, without resetting the firewall or interrupting service.

To connect to the web-based manager, you require:

- a computer with an Ethernet connection
- Microsoft Internet Explorer version 6.0 or higher or any recent version of most popular web browser
- a crossover Ethernet cable or an Ethernet hub with two Ethernet cables



Note: Before starting Internet Explorer, (or any recent version of the most popular web browser), ping to your FortiWiFi unit to see if the connection between the computer and the FortiWiFi unit is working properly.

To connect to the web-based manager

- 1 Set the IP address of the computer with an Ethernet connection to the static IP address 192.168.1.2 with a netmask of 255.255.255.0.

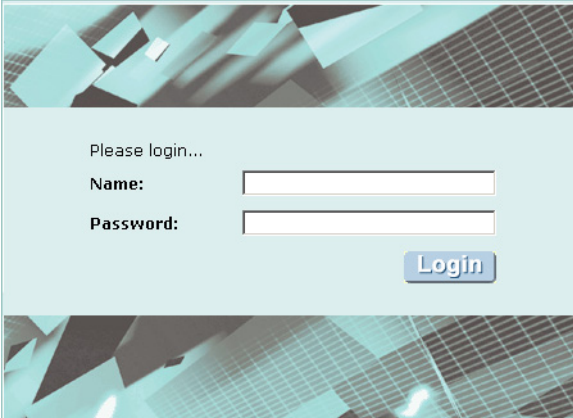
You can also configure the management computer to obtain an IP address automatically using the DHCP. The FortiWiFi DHCP server assigns the management computer an IP address in the range 192.168.1.1 to 192.168.1.254.

- 2 Using the crossover cable or the Ethernet hub and cables, connect the internal interface of the FortiWiFi unit to the computer Ethernet connection.
- 3 Start Internet Explorer and browse to the address <https://192.168.1.99>. (remember to include the “s” in https://).

To support a secure HTTPS authentication method, the FortiWiFi unit ships with a self-signed security certificate, and is offered to remote clients whenever they initiate a HTTPS connection to the FortiWiFi unit. When you connect, the FortiWiFi unit displays two security warnings in the browser.

The first warning prompts you to accept and optionally install the FortiWiFi unit's self-signed security certificate. If you do not accept the certificate, the FortiWiFi unit refuses the connection. If you accept the certificate, the FortiWiFi login page appears. The credentials entered are encrypted before they are sent to the FortiWiFi unit. If you choose to accept the certificate permanently, the warning is not displayed again.

Just before the FortiWiFi login page appears, a second warning informs you that the FortiWiFi certificate distinguished name differs from the original request. This warning occurs because the FortiWiFi unit redirects the connection. This is an informational message. Select OK to continue logging in.

Figure 2: FortiWiFi login


- 4 Type `admin` in the Name field and select Login.

System Dashboard

After logging into the web-based manager, the web browser displays the system dashboard. The dashboard provides you with all system status information in one location. For details on the information displayed on the dashboard, see the [FortiGate Administration Guide](#).

Command line interface

You can access the FortiWiFi command line interface (CLI) by connecting a management computer serial port to the FortiWiFi serial console connector. You can also use Telnet or a secure SSH connection to connect to the CLI from any network that is connected to the FortiWiFi unit, including the Internet.

The CLI supports the same configuration and monitoring functionality as the web-based manager. In addition, you can use the CLI for advanced configuration options that are not available from the web-based manager. This guide contains information about basic and advanced CLI commands. For a more complete description about connecting to and using the FortiWiFi CLI, see the [FortiGate CLI Reference](#).

Connecting to the CLI

As an alternative to the web-based manager, you can install and configure the FortiWiFi unit using the CLI. Configuration changes made with the CLI are effective immediately without resetting the firewall or interrupting service.

To connect to the FortiWiFi CLI you require:

- a computer with an available communications port
- the RJ-45 to DB-9 serial cable included in your FortiWiFi package
- terminal emulation software such as HyperTerminal for Microsoft Windows



Note: The following procedure uses Microsoft Windows HyperTerminal software. You can apply these steps to any terminal emulation program.

To connect to the CLI

- 1 Connect the RJ-45 to DB-9 serial cable/console port.
- 2 Start HyperTerminal, enter a name for the connection and select OK.
- 3 Configure HyperTerminal to connect directly to the communications port on your computer and select OK.
- 4 Select the following port settings and select OK:

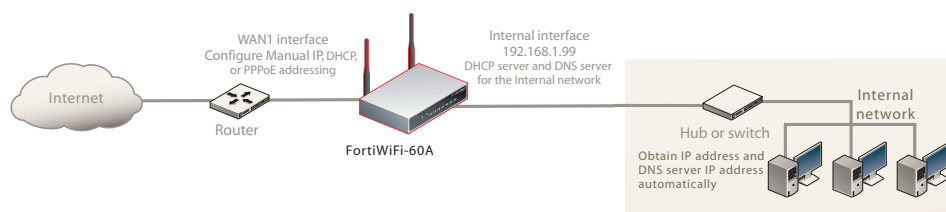
| | |
|------------------------|------|
| Bits per second | 9600 |
| Data bits | 8 |
| Parity | None |
| Stop bits | 1 |
| Flow control | None |
- 5 Press Enter to connect to the FortiWiFi CLI.
The login prompt appears.
- 6 Type `admin` and press Enter twice.
The following prompt is displayed:
Welcome !
Type `?` to list available commands. For information about how to use the CLI, see the [FortiGate CLI Reference](#).

Quick installation using factory defaults

You can quickly set up your FortiWiFi unit for a home or small office using the web-based manager and the factory default FortiWiFi configuration. All you need to do is set your network computers to obtain an IP address automatically and to obtain DNS server IP addresses automatically (using DHCP), access the web-based manager, and configure the required settings for the FortiWiFi WAN1 interface. You can also configure FortiWiFi DNS servers and add a FortiWiFi default route if needed.

The FortiWiFi internal interface acts as a DHCP server for the internal network, automatically assigning IP addresses to computers (up to 100 computers) in the range of 192.168.1.110 –192.168.1.210.

Figure 3: Quick configuration using default settings



The FortiWiFi DHCP server also assigns the DNS server IP address 192.168.1.99 to each computer on the internal network. As a result, the FortiWiFi unit internal interface acts as a DNS server for the internal network. Using DNS forwarding, the FortiWiFi unit forwards DNS requests received from the internal network to the DNS server IP addresses added to the FortiWiFi unit configuration and returns lookup results to the internal network.

For more information about default DHCP server settings see [“Factory default DHCP server configuration” on page 24](#).

The following procedure describes how to configure your internal network and the FortiWiFi unit to use the FortiWiFi default settings.

- 1 Connect the FortiWiFi unit between the internal network and the Internet and turn on the power.
- 2 Set the TCP/IP properties of the network computers to obtain an IP address automatically and a DNS server IP address automatically (using DHCP).
- 3 From the management computer, browse to <https://192.168.1.99>.
The FortiWiFi web-based manager appears.
- 4 Go to **System > Network > Interface** and select Edit for the WAN1 interface.
- 5 Select one of the following Addressing modes:
 - Manual: enter a static IP address and netmask, select OK, and go to step 6
 - DHCP: to get an IP address from the ISP select DHCP and go to step 9
 - PPPoE: to get an IP address from the ISP select PPPoE and go to step 9
- 6 Go to **System > Network > Options**.
- 7 Select one of the following DNS settings:
 - Obtain DNS server address automatically: select to get the DNS addresses from the ISP, select Apply
 - Use the following DNS server addresses: select and enter the DNS server addresses given to you by the ISP, select Apply
- 8 Go to **Router > Static**, edit route #1 and change Gateway to the default gateway IP address from the ISP and select OK.
Network configuration is complete. Proceed to [“Next steps” on page 43](#).
- 9 Select Retrieve default gateway from server and Override internal DNS options if your ISP supports them, select OK, and proceed to [“Next steps” on page 43](#).
Go to step 6 if you are not selecting these options.

Factory defaults

The FortiWiFi unit ships with a factory default configuration. The default configuration allows you to connect to and use the FortiWiFi web-based manager to configure the FortiWiFi unit onto the network. To configure the FortiWiFi unit onto the network you add an administrator password, change network interface IP addresses, add DNS server IP addresses, and, if required, configure basic routing.

If you plan to operate the FortiWiFi unit in Transparent mode, you can switch to Transparent mode from the factory default configuration and then configure the FortiWiFi unit onto the network in Transparent mode.

Once you complete the network configuration, you can perform additional configuration tasks such as setting system time, configuring virus and attack definition updates, and registering the FortiWiFi unit.

The factory default firewall configuration includes a single network address translation (NAT) policy that allows users on your internal network to connect to the external network, and stops users on the external network from connecting to the internal network. You can add more firewall policies to provide more control of the network traffic passing through the FortiWiFi unit.

The factory default protection profiles can be used to apply different levels of antivirus protection, web content filtering, spam filtering, and IPS to the network traffic that is controlled by firewall policies.

This section includes the following topics:

- [Factory default DHCP server configuration](#)
- [Factory default NAT/Route mode network configuration](#)
- [Factory default Transparent mode network configuration](#)
- [Factory default firewall configuration](#)
- [Restoring the default settings](#)

Factory default DHCP server configuration

Using the factory default DHCP server settings, you can quickly configure the internal network and the FortiWiFi unit. See [“Quick installation using factory defaults” on page 20](#).

Table 3: Factory default DHCP server configuration

| | |
|------------------------|-------------------------------|
| Name | internal_dhcp_server |
| Interface | Internal |
| Default Gateway | 192.168.1.99 |
| IP Range | 192.168.1.110 – 192.168.1.210 |
| Network Mask | 255.255.255.0 |
| Lease Duration | 7 days |
| DNS Server 1 | 192.168.1.99 |

Factory default NAT/Route mode network configuration

When the FortiWiFi unit is first powered on, it is running in NAT/Route mode and has the basic network configuration listed in [Table 4 on page 24](#). This configuration allows you to connect to the FortiWiFi unit web-based manager and establish the configuration required to connect the FortiWiFi unit to the network. In [Table 4 on page 24](#), HTTPS administrative access means you can connect to the web-based manager using HTTPS protocol through this interface. Ping administrative access means this interface responds to ping requests.

Table 4: Factory default NAT/Route mode network configuration

| | | |
|------------------------------|-------------------------------------------|----------------------------------------------------|
| Administrator account | User name: Password: | admin (none) |
| Internal interface | IP: Netmask: Administrative Access: | 192.168.1.99 255.255.255.0 HTTP, HTTPS, Ping |
| DMZ interface | IP: Netmask: Administrative Access: | 10.10.10.1 255.255.255.0 HTTPS, Ping |
| WAN1 interface | IP: Netmask: Administrative Access: | 192.168.100.99 255.255.255.0 Ping |
| WAN2 interface | IP: Netmask: Administrative Access: | 192.168.101.99 255.255.255.0 Ping |
| Modem interface | IP: Netmask: Administrative Access: | 0.0.0.0 0.0.0.0 |
| | IP: | 10.10.80.1 |

Table 4: Factory default NAT/Route mode network configuration (Continued)

| | | |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| WLAN | Netmask: | 255.255.255.0 |
| | Administrative Access: | Ping |
| Network Settings | Default Gateway (for default route) | 192.168.100.1 |
| | Default Route A default route consists of a default gateway and the name of the interface connected to the external network (usually the Internet). The default gateway directs all non-local traffic to this interface and to the external network. | |
| | Primary DNS Server | 65.39.139.53 |
| | Secondary DNS Server | 65.39.139.63 |

Factory default Transparent mode network configuration

In Transparent mode, the FortiWiFi unit has the default network configuration listed in [Table 5](#).

Table 5: Factory default Transparent mode network configuration

| | | |
|------------------------------|-----------------------|--------------|
| Administrator account | User name: | admin |
| | Password: | (none) |
| Management IP | IP: | 0.0.0.0 |
| | Netmask: | 0.0.0.0 |
| DNS | Primary DNS Server: | 65.39.139.53 |
| | Secondary DNS Server: | 65.39.139.63 |
| Administrative access | Internal | HTTPS, Ping |
| | DMZ | HTTPS, Ping |
| | WAN1 | Ping |
| | WAN2 | Ping |
| | WLAN | HTTPS, Ping |

Factory default firewall configuration

FortiWiFi firewall policies control how all traffic is processed by the FortiWiFi unit. Until firewall policies are added, no traffic can be accepted by or pass through the FortiWiFi unit. The factory default configuration contains one firewall policy that allows all traffic originating on the internal network to access the Internet. No other traffic is allowed through the FortiWiFi unit. To allow traffic through the FortiWiFi unit, you can add firewall policies. See the [FortiGate Administration Guide](#) for information about adding firewall policies.

The following firewall configuration settings are included in the default firewall configuration to make it easier to add firewall policies.

Table 6: Factory default firewall configuration

| Configuration setting | Name | Description |
|----------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Firewall policy | Internal -> External | Source: All Destination: All |
| Firewall address | All | Firewall address matches the source or destination address of any packet. |
| Pre-defined service | More than 50 predefined services | Select from any of the 50 pre-defined services to control traffic through the FortiWiFi unit that uses that service. |
| Recurring schedule | Always | The recurring schedule is valid at any time. |
| Protection Profiles | Strict, Scan, Web, Unfiltered | Control how the FortiWiFi unit applies virus scanning, web content filtering, spam filtering, and IPS. |

The factory default firewall configuration is the same in NAT/Route and Transparent mode.

Factory default protection profiles

Use protection profiles to apply different protection settings for traffic controlled by firewall policies. You can use protection profiles to:

- configure antivirus protection for HTTP, FTP, IMAP, POP3, and SMTP firewall policies
- configure Web filtering for HTTP firewall policies
- configure Web category filtering for HTTP firewall policies
- configure spam filtering for IMAP, POP3, and SMTP firewall policies
- enable the Intrusion Protection System (IPS) for all services
- enable content logging for HTTP, FTP, IMAP, POP3, and SMTP firewall policies

By using protection profiles, you can build protection configurations that can be applied to different types of firewall policies. This allows you to customize types and levels of protection for different firewall policies.

For example, while traffic between internal and external addresses might need strict protection, traffic between trusted internal addresses might need moderate protection. You can configure firewall policies for different traffic services to use the same or different protection profiles.

Protection profiles can be added to NAT/Route mode and Transparent mode firewall policies. The FortiWiFi unit comes preconfigured with four protection profiles.

| | |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Strict | To apply maximum protection to HTTP, FTP, IMAP, POP3, and SMTP traffic. You may not use the strict protection profile under normal circumstances but it is available if you have problems with viruses and require maximum screening. |
| Scan | To apply antivirus scanning and file quarantining to HTTP, FTP, IMAP, POP3, and SMTP content traffic. |
| Web | To apply antivirus scanning and web content blocking to HTTP content traffic. Add this protection profile to firewall policies that control HTTP traffic. |
| Unfiltered | To apply no scanning, blocking or IPS. Use if you do not want to apply content protection to content traffic. You can add this protection profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected. |

Restoring the default settings

You can revert to the factory default settings if you change a network setting and are unable to recover from it.



Caution: This procedure deletes all changes you have made to the FortiWiFi configuration and reverses the system to its original configuration, including resetting interface addresses.

Restoring the default settings using the web-based manager

To reset the default settings

- 1 Go to **System > Status**.
- 2 In the Unit Operation display, select Reset.

Restoring the default settings using the CLI

To reset the default settings enter the following command:

```
execute factoryreset
```


Configuring the FortiWiFi

This section provides an overview of the operating modes of the FortiWiFi unit. Before beginning to configure the FortiWiFi unit, you need to plan how to integrate the unit into your network. Your configuration plan is dependent on the operating mode you select: NAT/Route mode or Transparent mode.

This section includes the following topics:

- [Planning the FortiWiFi configuration](#)
- [NAT/Route mode installation](#)
- [Transparent mode installation](#)
- [Next steps](#)

Planning the FortiWiFi configuration

Before you configure the FortiWiFi unit, you need to plan how to integrate the unit into the network. Among other things, you must decide whether you want the unit to be visible to the network, which firewall functions you want it to provide, and how you want it to control the traffic flowing between its interfaces.

Your configuration plan depends on the operating mode you select. You can configure the FortiWiFi unit in one of two modes: NAT/Route mode (the default) or Transparent mode.

You can also configure the FortiWiFi unit and the network it protects using the default settings.

NAT/Route mode

In NAT/Route mode, the FortiWiFi unit is visible to the network. Like a router, all its interfaces are on different subnets. The following interfaces are available in NAT/Route mode:

Table 7: NAT/Route mode network segments

| FortiWiFi Unit | Internal Interface | External Interface | Other |
|----------------|--------------------|--------------------|------------------------|
| FortiWiFi-60A | Internal | WAN1 WAN2 | DMZ WLAN (Modem) |
| FortiWiFi-60AM | Internal | WAN1 WAN2 | DMZ WLAN (Modem) |

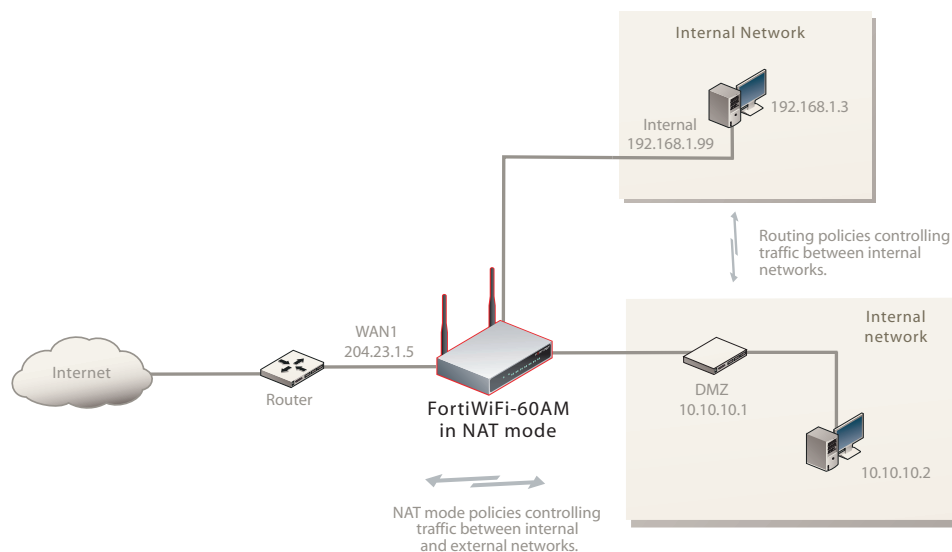
You can add firewall policies to control whether communications through the FortiWiFi unit operate in NAT or Route mode. Firewall policies control the flow of traffic based on the source address, destination address, and service of each packet. In NAT mode, the FortiWiFi unit performs network address translation before it sends the packet to the destination network. In Route mode, there is no address translation.

You typically use NAT/Route mode when the FortiWiFi unit is operating as a gateway between private and public networks. In this configuration, you would create NAT mode firewall policies to control traffic flowing between the internal, private network and the external, public network (usually the Internet).



Note: If you have multiple internal networks, such as a DMZ network in addition to the internal, private network, you could create route mode firewall policies for traffic flowing between them.

Figure 4: Example NAT/Route mode network configuration.



NAT/Route mode with multiple external network connections

In NAT/Route mode, you can configure the FortiWiFi unit with multiple redundant connections to the Internet.

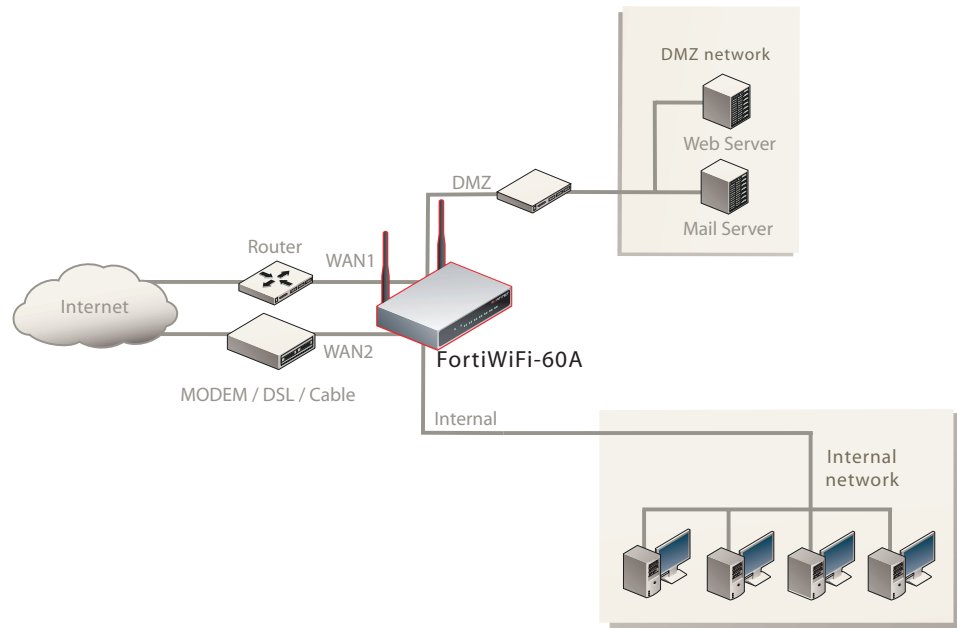
For example, you could create the following configuration:

- WAN1 is the default interface to the external network (usually the Internet)
- WAN2 is the redundant interface to the external network
- DMZ is interface to the DMZ network
- Internal is the interface to the internal network

You must configure routing to support redundant Internet connections. Routing can automatically redirect connections from an interface if its connection to the external network fails.

Otherwise, security policy configuration is similar to a NAT/Route mode configuration with a single Internet connection. You would create NAT mode firewall policies to control traffic flowing between the internal, private network and the external, public network (usually the Internet).

Figure 5: Example NAT/Route multiple internet connection



Transparent mode

In Transparent mode, the FortiWiFi unit is invisible to the network. Similar to a network bridge, all FortiWiFi interfaces must be on the same subnet. You only have to configure a management IP address so that you can make configuration changes. The management IP address is also used for antivirus and attack definition updates.

You typically use the FortiWiFi unit in Transparent mode on a private network behind an existing firewall or behind a router. The FortiWiFi unit performs firewall functions, IPSec VPN, virus scanning, IPS web content filtering, and Spam filtering.

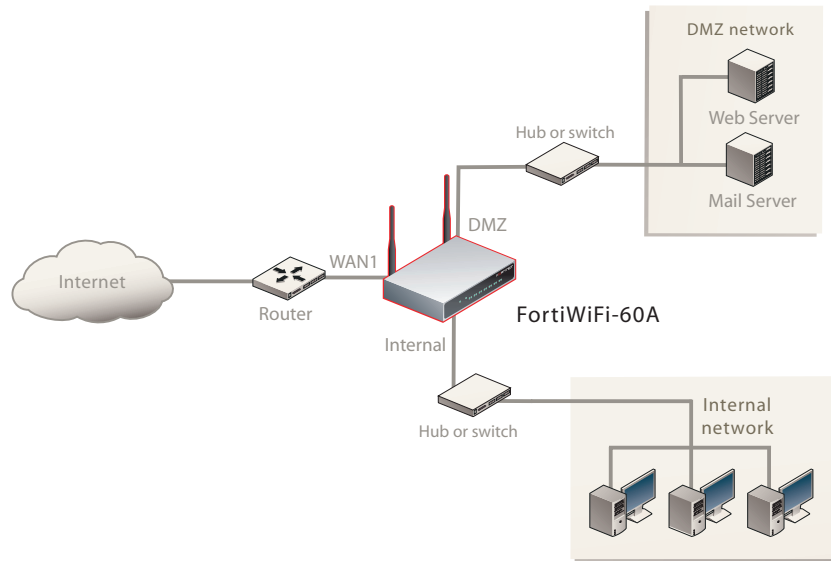
You can connect up to four network segments to the FortiWiFi unit to control traffic between these network segments.

Table 8: Transparent mode network segments

| FortiWiFi Unit | Internal Interface | External Interface | Other |
|----------------|-----------------------|--------------------|---------------------|
| FortiWiFi-60A | Internal (1, 2, 3, 4) | WAN1 | WAN2 DMZ WLAN |
| FortiWiFi-60AM | Internal (1, 2, 3, 4) | WAN1 | WAN2 DMZ WLAN |



Note: In Transparent mode, the modem interface is not available FortiWiFi-60AM.

Figure 6: Example Transparent mode network configuration.

NAT/Route mode installation

This section describes how to install the FortiWiFi unit in NAT/Route mode. This section includes the following topics:

- [Preparing to configure the FortiWiFi unit in NAT/Route mode](#)
- [DHCP or PPPoE configuration](#)
- [Using the web-based manager](#)
- [Using the command line interface](#)
- [Connecting the FortiWiFi unit to the network\(s\)](#)
- [Configuring the networks](#)

Preparing to configure the FortiWiFi unit in NAT/Route mode

Use [Table 9 on page 33](#) to gather the information you need to customize NAT/Route mode settings.

You can configure the FortiWiFi unit in two ways:

- The web-based manager GUI is a complete interface for configuring most settings. See [“Using the web-based manager” on page 33](#).
- The command line interface (CLI) is a complete text-based interface for configuring all settings. See [“Using the command line interface” on page 35](#).

The method you choose depends on the complexity of the configuration, access and equipment, and the type of interface you are most comfortable using.

Table 9: NAT/Route mode settings

| | | |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Administrator Password: | | |
| Internal | IP: | ____.____.____.____ |
| | Netmask: | ____.____.____.____ |
| WAN1 | IP: | ____.____.____.____ |
| | Netmask: | ____.____.____.____ |
| WAN2 | IP: | ____.____.____.____ |
| | Netmask: | ____.____.____.____ |
| DMZ | IP: | ____.____.____.____ |
| | Netmask: | ____.____.____.____ |
| WLAN | IP: | ____.____.____.____ |
| | Netmask: | ____.____.____.____ |
| Network settings | Default Gateway: | ____.____.____.____ |
| | (Interface connected to external network) | |
| | A default route consists of a default gateway and the name of the interface connected to the external network (usually the Internet). The default gateway directs all non-local traffic to this interface and to the external network. | |
| | Primary DNS Server: | ____.____.____.____ |
| | Secondary DNS Server: | ____.____.____.____ |

DHCP or PPPoE configuration

You can configure any FortiWiFi interface to acquire its IP address from a DHCP or PPPoE server. Your Internet Service Provider (ISP) may provide IP addresses using one of these protocols.

To use the FortiWiFi DHCP server, you need to configure an IP address range and default route for the server. No configuration information is required for interfaces that are configured to use DHCP.

PPPoE requires you to supply a user name and password. In addition, PPPoE unnumbered configurations require you to supply an IP address. Use [Table 10](#) to record the information you require for your PPPoE configuration.

Table 10: PPPoE setting

| | |
|-------------------|--|
| User name: | |
| Password: | |

Using the web-based manager

You can use the web-based manager for the initial configuration of the FortiWiFi unit and all FortiWiFi unit settings.

For information about connecting to the web-based manager, see [“Connecting to the web-based manager”](#) on page 18.

Configuring basic settings

After connecting to the web-based manager, you can use the following procedures to complete the basic configuration of the FortiWiFi unit.

To add/change the administrator password

- 1 Go to **System > Admin > Administrators**.
- 2 Select the Change Password icon for the admin administrator.
- 3 Enter the new password and enter it again to confirm.
- 4 Select OK.

To configure interfaces

- 1 Go to **System > Network > Interface**.
- 2 Select the edit icon for an interface.
- 3 Set the addressing mode for the interface.
Choose from manual, DHCP, or PPPoE.
- 4 Complete the addressing configuration.
 - For manual addressing, enter the IP address and netmask for the interface.
 - For DHCP addressing, select DHCP and any required settings.
 - For PPPoE addressing, select PPPoE, and enter the username and password and any other required settings.

For information about how to configure these and other interface settings, see the FortiWiFi online help or the [FortiGate Administration Guide](#).

- 5 Select OK.
- 6 Repeat this procedure for each interface.



Note: If you change the IP address of the interface you are connecting to, you must connect through a web browser again using the new address. Browse to https:// followed by the new IP address of the interface. If the new IP address of the interface is on a different subnet, you may have to change the IP address of your computer to the same subnet.

To configure DNS server settings

- 1 Go to **System > Network > Options**.
- 2 Enter the IP address of the primary DNS server.
- 3 Enter the IP address of the secondary DNS server.
- 4 Select Apply.

Adding a default route

Add a default route to configure where the FortiWiFi unit sends traffic destined for an external network (usually the Internet). Adding the default route also defines which interface is connected to an external network. The default route is not required if the interface connected to the external network is configured using DHCP or PPPoE.

To add a default route

- 1 Go to **Router > Static**.
- 2 If the Static Route table contains a default route (IP and Mask set to 0.0.0.0), select the Delete icon to delete this route.
- 3 Select Create New.
- 4 Set Destination IP to 0.0.0.0.
- 5 Set Mask to 0.0.0.0.
- 6 Set Gateway to the default gateway IP address.
- 7 Set Device to the interface connected to the external network.
- 8 Select OK.

Verifying the web-based manager configuration

To verify access settings, go to the interface you want to verify and select the edit icon. The Administrative Access field should have check marks beside the settings you chose in the preceding steps.

Verify the connection

To verify your connection, try the following:

- browse to www.fortinet.com
- retrieve or send email from your email account

If you cannot browse to the web site or retrieve/send email from your account, review the previous steps to ensure all information was entered correctly and try again.

Using the command line interface

You can also configure the FortiWiFi unit using the command line interface (CLI). For information about connecting to the CLI, see [“Connecting to the CLI” on page 19](#).

Configuring the FortiWiFi unit to operate in NAT/Route mode

Use the information you gathered in [Table 9 on page 33](#) to complete the following procedures.

To add/change the administrator password

- 1 Log in to the CLI.
- 2 Change the admin administrator password. Enter:

```
config system admin
  edit admin
    set password <psswr>
  end
```

To configure interfaces

- 1 Log into the CLI.
- 2 Set the IP address and netmask of the internal interface to the internal IP address and netmask you recorded in [Table 9 on page 33](#). Enter:

```
config system interface
  edit internal
    set mode static
    set ip <address_ip> <netmask>
  end
```

Example

```
config system interface
  edit internal
    set mode static
    set ip <192.168.120.99> <255.255.255.0>
  end
```

- 3 Set the IP address and netmask of the external interface to the external IP address and netmask you recorded in [Table 9 on page 33](#).

```
config system interface
  edit <interface>
    set mode static
    set ip <address_ip> <netmask>
  end
```

Example

```
config system interface
  edit wan1
    set mode static
    set ip <204.23.1.5> <255.255.255.0>
  end
```

To set the WAN1 interface to use DHCP, enter:

```
config system interface
  edit wan1
    set mode dhcp
  end
```

To set the WAN1 interface to use PPPoE, enter:

```
config system interface
  edit WAN1
    set mode pppoe
    set connection enable
    set username <name_str>
    set password <psswr>
  end
```

- 4 Use the same syntax to set the IP address of each FortiWiFi interface as required.
- 5 Confirm that the addresses are correct. Enter:

```
get system interface
```

The CLI lists the IP address, netmask, and other settings for each of the FortiWiFi interfaces.

To configure DNS server settings

Set the primary and secondary DNS server IP addresses. Enter

```
config system dns
  set primary <address_ip>
  set secondary <address_ip>
end
```

Example

```
config system dns
  set primary 293.44.75.21
  set secondary 293.44.75.22
end
```

Adding a default route

Add a default route to configure where the FortiWiFi unit sends traffic that should be sent to an external network (usually the Internet). Adding the default route also defines which interface is connected to an external network. The default route is not required if the interface connected to the external network is configured using DHCP or PPPoE.

To add a default route

Set the default route to the Default Gateway IP address. Enter:

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway <gateway_IP>
    set device <interface>
  end
```

Example

If the default gateway IP is 204.23.1.2 and this gateway is connected to WAN1:

```
config router static
edit 1
set dst 0.0.0.0 0.0.0.0
set gateway 204.23.1.2
set device wan1
end
```

Verify the connection

To verify the connection, try the following:

- ping the FortiWiFi unit
- browse to the web-based manager GUI
- retrieve or send email from your email account

If you cannot browse to the web site or retrieve/send email from your account, review the previous steps to ensure all information was entered correctly and try again.

You are now finished the initial configuration of the FortiWiFi unit.

Connecting the FortiWiFi unit to the network(s)

When you have completed the initial configuration, you can connect the FortiWiFi unit between your internal network and the Internet.

The following network connections are available on the FortiWiFi unit:

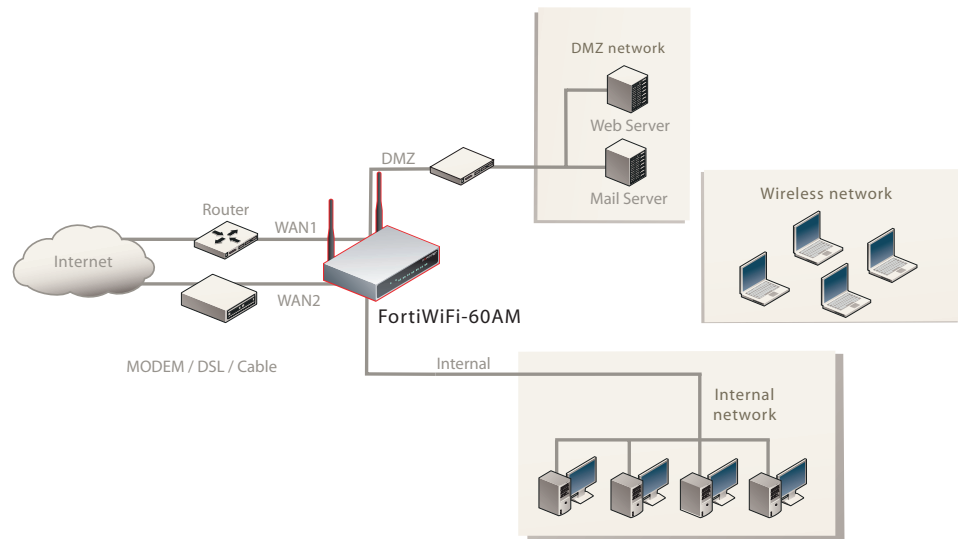
- Internal for connecting to your internal network
- WAN1 for connecting to the Internet
- WLAN is the interface to the wireless LAN on the FortiWiFi models
- WAN2 is the interface to an external network
- DMZ is the interface to the DMZ network

To connect the FortiWiFi unit

- 1** Connect the Internal interface to the hub or switch connected to your internal network.
- 2** Connect the WAN1 interface to the Internet.
Connect to the public switch or router provided by your Internet Service Provider. If you are a DSL or cable subscriber, connect the WAN1 interface to the internal or LAN connection of your DSL or cable modem.
- 3** Optionally connect the DMZ interface to your DMZ network.

You can use a DMZ network to provide access from the Internet to a web server or other server without installing the servers on your internal network.

Figure 7: NAT/Route mode connections



Configuring the networks

If you are running the FortiWiFi unit in NAT/Route mode, your networks must be configured to route all Internet traffic to the IP address of the interface where the networks are connected.

- For the internal network, change the default gateway address of all computers and routers connected directly to your internal network to the IP address of the FortiWiFi internal interface.
- For the DMZ network, change the default gateway address of all computers and routers connected directly to your DMZ network to the IP address of the FortiWiFi DMZ interface.
- For the WAN network, change the default gateway address of all computers and routers connected to your WAN network to the IP address of the FortiWiFi WAN interface.
- For the WLAN network, configure an IP address for the wireless local area network interface.

If you are using the FortiWiFi unit as the DHCP server for your internal network, configure the computers on your internal network for DHCP.

Make sure the connected FortiWiFi unit is functioning properly by connecting to the Internet from a computer on the internal network. You should be able to connect to any Internet address.

Transparent mode installation

This section describes how to install the FortiWiFi unit in Transparent mode. This section includes the following topics:

- [Preparing to configure Transparent mode](#)
- [Using the web-based manager](#)
- [Using the Command line interface](#)
- [Connecting the FortiWiFi unit to your network](#)

Preparing to configure Transparent mode

Use [Table 11 on page 40](#) to gather the information you need to customize Transparent mode settings.

You can configure Transparent mode using one of the following methods:

- the web-based manager GUI
- the command line interface (CLI)

The method you choose depends on the complexity of the configuration, access and equipment, and the type of interface you are most comfortable using.

Table 11: Transparent mode settings

| | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------------|
| Administrator Password: | | |
| Management IP | IP: | ____ . ____ . ____ . ____ |
| | Netmask: | ____ . ____ . ____ . ____ |
| | Default Gateway: | ____ . ____ . ____ . ____ |
| The management IP address and netmask must be valid for the network from which you will manage the FortiWiFi unit. Add a default gateway if the FortiWiFi unit must connect to a router to reach the management computer. | | |
| DNS Settings | Primary DNS Server: | ____ . ____ . ____ . ____ |
| | Secondary DNS Server: | ____ . ____ . ____ . ____ |

Using the web-based manager

You can use the web-based manager to complete the initial configuration of the FortiWiFi unit. You can continue to use the web-based manager for all FortiWiFi unit settings.

For information about connecting to the web-based manager, see [“Connecting to the web-based manager” on page 18](#).

The first time you connect to the FortiWiFi unit, it is configured to run in NAT/Route mode.

To switch to Transparent mode using the web-based manager

- 1 Go to **System > Status**.
- 2 Select Change beside the Operation Mode.
- 3 Select Transparent in the Operation Mode list.
- 4 Type the Management IP/Netmask address and Default Gateway address you gathered in [Table 11 on page 40](#).
- 5 Select Apply.

You do not have to reconnect to the web-based manager at this time. Once you select Apply, the changes are immediate, and you can go to the system dashboard to verify the FortiWiFi unit has changed to Transparent mode.

To configure DNS server settings

- 1 Go to **System > Network > Options**.
- 2 Enter the IP address of the primary DNS server.
- 3 Enter the IP address of the secondary DNS server.
- 4 Select Apply.

Using the Command line interface

As an alternative to the web-based manager, you can begin the initial configuration of the FortiWiFi unit using the command line interface (CLI). To connect to the CLI, see [“Connecting to the CLI” on page 19](#). Use the information you gathered in [Table 11 on page 40](#) to complete the following procedures.

To change to Transparent mode using the CLI

- 1 Make sure you are logged into the CLI.
- 2 Switch to Transparent mode. Enter:

```
config system settings
    set opmode transparent
    set manageip <address_ip> <netmask>
    set gateway <address_gateway>
end
```

After a few seconds, the following prompt appears:

```
Changing to TP mode
```

- 3 When the login prompt appears, enter the following:

```
get system settings
```

The CLI displays the status of the FortiWiFi unit including the management IP address and netmask:

```
opmode          : transparent
manageip        : <address_ip><netmask>
```

You should verify the DNS server settings are correct. The DNS settings carry over from NAT/Route mode and may not be correct for your specific Transparent mode configuration. Use [Table 11 on page 40](#) to configure the DNS server settings.

To verify the DNS server settings

Enter the following commands to verify the FortiWiFi unit's DNS server settings:

```
show system dns
```

The above CLI command should give you the following DNS server setting information:

```
config system dns
  set primary 293.44.75.21
  set secondary 293.44.75.22
  set fwdintf internal
end
```

To configure DNS server settings

Set the primary and secondary DNS server IP addresses. Enter:

```
config system dns
  set primary <address_ip>
  set secondary <address_ip>
end
```

Example

```
config system dns
  set primary 293.44.75.21
  set secondary 293.44.75.22
end
```

Reconnecting to the web-based manager

When the FortiWiFi unit has switched to Transparent mode, you can reconnect to the web-based manager using the new IP address. Browse to <https://> followed by the new IP address. If you connect to the management interface through a router, make sure you have added a default gateway for that route to the management IP default gateway field.

Connecting the FortiWiFi unit to your network

When you complete the initial configuration, you can connect the FortiWiFi unit between your internal network and the Internet and connect an additional network to the DMZ interface.



Note: You cannot use the modem interface as a redundant Internet connection when running in Transparent mode.

To connect the FortiWiFi unit running in Transparent mode:

- 1 Connect the Internal interface to the hub or switch connected to your internal network.
- 2 Connect the WAN1 interface to network segment connected to the external firewall or router.
Connect to the public switch or router provided by your Internet Service Provider.
- 3 Connect the DMZ interface to another network.

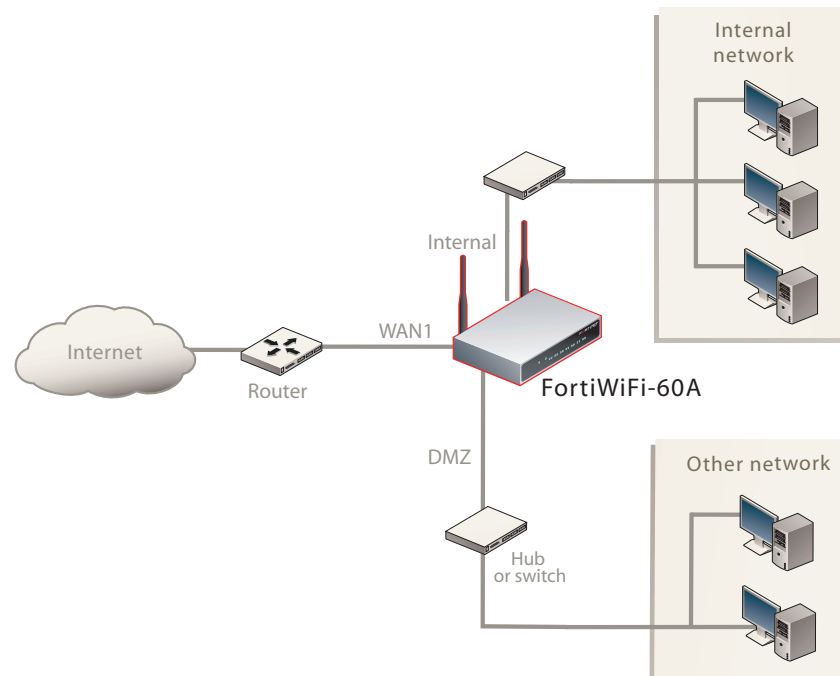
Verify the connection

To verify the connection, try the following:

- ping the FortiWiFi unit
- browse to the web-based manager GUI
- retrieve or send email from your email account

If you cannot browse to the web site or retrieve/send email from your account, review the previous steps to ensure all information was entered correctly and try again.

Figure 8: Transparent mode connections



Next steps

You can use the following information to configure FortiWiFi system time, and to configure antivirus and attack definition updates.

Refer to the [FortiGate Administration Guide](#) for complete information on configuring, monitoring, and maintaining your FortiWiFi unit.

Set the date and time

For effective scheduling and logging, the FortiWiFi system date and time must be accurate. You can either manually set the system date and time or configure the FortiWiFi unit to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the date and time

- 1 Go to **System > Status**.
- 2 Under **System Information > System Time**, select **Change**.
- 3 Select **Refresh** to display the current FortiWiFi system date and time.
- 4 Select your **Time Zone** from the list.
- 5 Optionally, select **Automatically adjust clock for daylight saving changes** check box.
- 6 Select **Set Time** and set the FortiWiFi system date and time.

- 7 Set the hour, minute, second, month, day, and year as required.
- 8 Select OK.



Note: If you choose the option Automatically adjust clock for daylight saving changes, the system time must be manually adjusted after daylight savings time ends.

To use NTP to set the FortiWiFi date and time

- 1 Go to **System > Status**.
- 2 Under **System Information > System Time**, select Change.
- 3 Select Synchronize with NTP Server to configure the FortiWiFi unit to use NTP to automatically set the system time and date.
- 4 Enter the IP address or domain name of the NTP server that the FortiWiFi unit can use to set its time and date.
- 5 Specify how often the FortiWiFi unit should synchronize its time with the NTP server.
- 6 Select OK.

Updating antivirus and IPS signatures

You can configure the FortiWiFi unit to connect to the FortiGuard Distribution Network (FDN) to update the antivirus (including grayware), antispam and IPS attack definitions.

The FDN is a world wide network of FortiGuard Distribution Servers (FDS). When the FortiWiFi unit connects to the FDN, it connects to the nearest FDS. To do this, all FortiWiFi units are programmed with a list of FDS addresses sorted by nearest time zone according to the time zone configured for the FortiWiFi unit.

You can update your antivirus and IPS signatures using the web-based manager or the CLI. Before you can begin receiving updates, you must register your FortiWiFi unit from the Fortinet web page.



Note: Update AV and IPS signatures on a regular basis. If you do not update AV and IPS signatures regularly, the FortiWiFi unit can become vulnerable to new viruses.

After registering your FortiWiFi unit, verify the FortiWiFi unit can connect to the FDN:

- Check that the FortiWiFi unit's system time is correct.
- From the web-based manager, select refresh from the FortiGuard Center.

If you cannot connect to the FDN, follow the procedure for registering your FortiWiFi unit and try again or see [“Adding an override server” on page 46](#).

Updating antivirus and IPS signatures from the web-based manager

After you have registered your FortiWiFi unit, you can update antivirus and IPS signatures using the web-based manager. The FortiGuard Center enables you to receive push updates, allow push update to a specific IP address, and schedule updates for daily, weekly, or hourly intervals.

To update antivirus definitions and IPS signatures

- 1 Go to **System > Maintenance > FortiGuard Center**.
- 2 Select the blue arrow for AntiVirus and IPS Downloads to expand the options.
- 3 Select Update Now to update the antivirus definitions.

If the connection to the FDN is successful, the web-based manager displays a message similar to the following:

```
Your update request has been sent. Your database will
be updated in a few minutes. Please check your update
page for the status of the update.
```

After a few minutes, if an update is available, the System FortiGuard Center page lists new version information for antivirus definitions. The System Status page also displays new dates and version numbers for the antivirus definitions. Messages are recorded to the event log indicating whether the update was successful or not.



Note: Updating antivirus definitions can cause a very short disruption in traffic currently being scanned while the FortiWiFi unit applies the new signature database. Schedule updates when traffic is light, for example overnight, to minimize any disruption.

Updating the IPS signatures from the CLI

You can update IPS signatures using the CLI. Use the following procedure to update IPS signatures.



Note: You can only update antivirus definitions from the web-based manager.

To update IPS signatures using the CLI

- 1 Log into the CLI.
- 2 Enter the following CLI command:

```
configure system autoupdate ips
  set accept-recommended-settings enable
end
```

Scheduling antivirus and IPS updates

You can schedule regular, automatic updates of antivirus and IPS signatures, either from the web-based manager or the CLI.

To enable schedule updates from the web-based manager

- 1 Go to **System > Maintenance > FortiGuard Center**.
- 2 Select the blue arrow for AntiVirus and IPS Downloads to expand the options.
- 3 Select the Scheduled Update check box.
- 4 Select one of the following to check for and download updates.

Every Once every 1 to 23 hours. Select the number of hours and minutes between each update request.

| | |
|---------------|----------------------------------------------------------------------------------------|
| Daily | Once a day. You can specify the time of day to check for updates. |
| Weekly | Once a week. You can specify the day of the week and time of day to check for updates. |

5 Select Apply.

The FortiWiFi unit starts the next scheduled update according to the new update schedule.

Whenever the FortiWiFi unit runs a scheduled update, the event is recorded in the FortiWiFi event log.

To enable schedule updates from the CLI

- 1 Log into the CLI.
- 2 Enter the following command:

```
config system autoupdate schedule
  set day
  set frequency
  set status
  set time
end
```

Example

```
config system autoupdate schedule
  set update every Sunday
  set frequency weekly
  set status enable
  set time 16:45
end
```

Adding an override server

If you cannot connect to the FDN, or if your organization provides updates using their own FortiGuard server, use the following procedures to add the IP address of an override FortiGuard server in either the web-based manager or the CLI.

To add an override server from the web-based manager

- 1 Go to **System > Maintenance > FortiGuard Center**.
- 2 Select the blue arrow for AntiVirus and IPS Downloads to expand the options.
- 3 Select the Use override server address check box.
- 4 Type the fully qualified domain name or IP address of a FortiGuard server.
- 5 Select Apply.

The FortiWiFi unit tests the connection to the override server.

If the FDN setting changes to available, the FortiWiFi unit has successfully connected to the override server.

If the FDN stays set to not available, the FortiWiFi unit cannot connect to the override server. Check the FortiWiFi configuration and network configuration for settings that would prevent the FortiWiFi unit from connecting to the override FortiGuard server.

To add an override server using the CLI

- 1 Log into the CLI.
- 2 Enter the following command:

```
config system autoupdate override
    set address
    set status
end
```


Configuring the modem interface

This section describes how to configure the FortiWiFi-60AM internal modem using the web-based manager and the FortiWiFi-60A with an external modem using the Command Line interface (CLI).

The FortiWiFi-60A/AM series supports a redundant or stand alone modem interface in NAT/Route mode.

- In redundant mode, the modem interface automatically takes over from a selected Ethernet interface when that Ethernet interface is unavailable.
- In stand alone mode, the modem interface is the connection from the FortiWiFi unit to the Internet.

When connecting to an ISP in either configuration, the modem can automatically dial up to three dial-up accounts until the modem connects to an ISP.

This section includes the following topics:

- [Selecting a modem mode](#)
- [Configuring modem settings](#)
- [Connecting and disconnecting the modem in Stand alone mode](#)
- [Configuring the modem using the CLI](#)
- [Adding a Ping Server](#)
- [Adding firewall policies for modem connections](#)

Selecting a modem mode

The modem interface can work in one of two modes:

- redundant mode
- stand alone mode

Redundant mode configuration

The redundant modem interface serves as a backup to the Ethernet interface. If that Ethernet interface disconnects from its network, the modem automatically dials the configured dial-up account(s). When the modem connects to a dial-up account, the FortiWiFi unit routes IP packets normally destined for the selected Ethernet interface to the modem interface. During this time, the unit pings the Ethernet connection to check when it is back online.

When the Ethernet interface can connect to its network again, the FortiWiFi unit disconnects the modem interface and switches back to the Ethernet interface.

For the FortiWiFi unit to switch from an Ethernet interface to the modem, you must select the name of the interface in the modem configuration and configure a ping server for that interface. You must also configure firewall policies for connections between the modem interface and other FortiWiFi interfaces.

To configure a redundant modem connection for the FortiWiFi-60AM

- 1 Go to **System > Network > Modem**.
- 2 Select Enable modem.
- 3 Select Redundant for the mode.
- 4 From the Redundant for list, select the Ethernet interface you want the modem to back up.
- 5 Configure other modem settings as required.
[“Configuring modem settings” on page 52.](#)
- 6 Configure a ping server for the Ethernet interface selected in step 4.
[See “Adding a Ping Server” on page 56.](#)
- 7 Configure firewall policies for connections to the modem interface.
[See “Adding firewall policies for modem connections” on page 56.](#)

To configure the FortiWiFi-60A using the CLI

- 1 Log into the CLI.
- 2 Enter the following to configure a redundant modem:

```
config system modem
    set status enable
    set status mode redundant
end
```

Stand alone mode configuration

In stand alone mode, you manually connect the modem to a dial-up account. The modem interface operates as the primary connection to the Internet. The FortiWiFi unit routes traffic through the modem interface, which remains permanently connected to the dial-up account.

If the connection to the dial-up account fails, the FortiWiFi unit modem automatically redials the number. The modem redials the ISP number based on the amount of times specified by the redial limit, or until it connects to a dial-up account.

In stand alone mode the modem interface replaces the external Ethernet interface. You must also configure firewall policies for connections between the modem interface and other FortiWiFi interfaces.



Note: Do not add a default route to the Ethernet interface that the modem interface replaces.



Note: Do not add firewall policies for connections between the Ethernet interface that the modem replaces and other interfaces.

To operate in stand alone mode for the FortiWiFi-60AM

- 1 Go to **System > Network > Modem**.
- 2 Configure other modem settings as required.

See [“Configuring modem settings” on page 52](#).

Make sure there is correct information in one or more Dial-up Accounts.

- 3 Configure firewall policies for connections to the modem interface.
See [“Adding firewall policies for modem connections” on page 56](#).
- 4 Select Dial Up.

The FortiWiFi unit initiates dialing into each dial-up account in turn until the modem connects to an ISP.

To operate in stand alone mode for the FortiWiFi-60A on the CLI

- 1 Log into the CLI.
- 2 Enter the following to configure a stand alone modem:

```
config system modem
    set status enable
    set status mode standalone
end
```

- 3 Enter the following to configure the dialup account:

```
config system modem
    set auto-dial
    set idle-timeout <minutes_interger>
    set passwd1 <passwd_srt>
    set phone1 <phone-number_str>
    set redial <tries_interger>
    set username1 <name_str>
end
```

Configuring modem settings

Configure modem settings so that the FortiWiFi unit uses the modem to connect to your ISP dial-up accounts. You can configure the modem to connect up to three dial-up accounts. You can also enable and disable FortiWiFi modem support, configure what the modem dials, and select the FortiWiFi interface that the modem is redundant for.

Figure 9: Modem settings (Stand alone and Redundant)

The figure shows two side-by-side screenshots of the FortiWiFi modem settings web interface. Both screenshots show the 'Enable Modem' checkbox checked and the modem status as 'not active'.
 The left screenshot is for 'Stand alone' mode. It features a 'Dial Now' button, an 'Auto-dial' checkbox, a 'Dial on demand' checkbox, and an 'Idle timeout' of 5 minutes. The 'Redial Limit' is set to 'None'. There are three 'Dialup Account' sections, each with fields for Phone Number, User Name, and Password.
 The right screenshot is for 'Redundant' mode. It features a 'Dial on demand' checkbox, an 'Idle timeout' of 5 minutes, a 'Redundant for' dropdown menu set to '1', a 'Holddown Timer' of 60 seconds, and a 'Redial Limit' set to 'None'. It also has three 'Dialup Account' sections with fields for Phone Number, User Name, and Password.
 Both screenshots have an 'Apply' button at the bottom.

| | |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Modem | Select to enable the modem. |
| Modem status | The modem status shows one of the following: “not active”, “connecting”, “connected”, “disconnecting” or “hung up” (Stand alone mode only). |
| Dial Now/Hang Up | (Stand alone mode only) Select Dial Now to manually connect to a dial-up account. If the modem is connected, you can select Hang Up to manually disconnect the modem. |
| Mode | Select Stand alone or Redundant mode. In Stand alone mode, the modem is an independent interface. In Redundant mode, the modem is a backup facility for a selected Ethernet interface. |
| Auto-dial | (Stand alone mode only) Select to dial the modem automatically if the connection is lost or the FortiWiFi unit is restarted. You cannot select Auto-dial if Dial on demand is selected. |
| Redundant for | (Redundant mode only) Select the Ethernet interface the modem provides backup service. |
| Dial on demand | Select to dial the modem when packets are routed to the modem interface. The modem disconnects after the idle timeout period if there is no network activity. When traffic occurs on the interface, the FortiGate unit dials the modem again. In Standalone mode, you cannot select Dial on demand if Auto-dial is selected. |
| Idle timeout | (Stand alone mode only) Enter the timeout duration in minutes. After this period of inactivity, the modem disconnects. |
| Holddown Timer | (Redundant mode only) Enter the time (1-60 seconds) the FortiWiFi unit waits before switching from the modem interface to the primary interface, after the primary interface has been restored. Configure a higher value if you find the FortiWiFi unit switching repeatedly between the primary interface and the modem interface. |
| Redial Limit | The maximum number of times (1-10) the FortiWiFi unit modem attempts to reconnect to the ISP if the connection fails. Select None to have no limit on redial attempts. |

| | |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dialup Account | Configure up to three dial-up accounts. The FortiWiFi unit tries connecting to each account in order until a connection can be established. |
| Phone Number | The phone number required to connect to the dialup account. Do not add spaces to the phone number. Make sure to include standard special characters for pauses, country codes, and other functions as required by your modem to connect to your dialup account. |
| User Name | The user name (maximum 63 characters) sent to the ISP. |
| Password | The password sent to the ISP. |

You can configure and use the modem in NAT/Route mode only.

To configure modem settings

- 1 Go to **System > Network > Modem**.
- 2 Select Enable Modem.
- 3 Change any of the dial-up connection settings.
- 4 Enter the settings for Dial-up Account 1 settings.
- 5 If you have multiple dial-up accounts, enter Phone Number, User Name, and Password for Dial-up Account 2 and Dial-up Account 3.
- 6 Select Apply.

Connecting and disconnecting the modem in Stand alone mode

To connect to a dial-up account

- 1 Go to **System > Network > Modem**.
- 2 Select Enable Modem.
- 3 Make sure there is correct information in one or more Dial-up Accounts.
- 4 Select Apply if you make any configuration changes.
- 5 Select Dial Now.

The FortiWiFi unit initiates dialing into each dial-up account in turn until the modem connects to an ISP.

not active The modem interface is not connected to the ISP.

active The modem interface is attempting to connect to the ISP, or is connected to the ISP.

A green check mark indicates the active dial-up account.

The IP address and netmask are assigned to the modem interface. Go to **System > Network > Interface** to verify the IP address and netmask.

To disconnect the modem

Use the following procedure to disconnect the modem from a dial-up account.

- 1 Go to **System > Network > Modem**.
- 2 Select Hang Up if you want to disconnect from the dial-up account.

Configuring the modem using the CLI

Configure the modem settings for the FortiWiFi-60A/AM through the CLI. The following table of CLI commands are specifically for the modem configuration.

| Keywords and variables | Description | Default |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| altmode {enable disable} | Enable for installations using PPP in China. | enable |
| auto-dial {enable disable} | Enable to dial the modem automatically if the connection is lost, or the FortiWiFi unit is restarted. dial-on-demand must be disabled. mode must be standalone | disable |
| connect_timeout <seconds> | Set the connection completion timeout (30-255 seconds). | 90 |
| dial-on-demand {enable disable} | Enable to dial the modem when packets are routed to the modem interface. The modem disconnects after the idle-timer period. auto-dial must be disabled. When traffic occurs on the interface, the FortiGate unit dials the modem again. | disable |
| holddown-timer <seconds> | Used only when the modem is configured as a backup for an interface. Set the time (1-60 seconds) that the FortiWiFi unit waits before switching from the modem interface to the primary interface, after the primary interface has been restored. mode must be redundant. | 60 |
| idle-timer <minutes> | Set the number of minutes the modem connection can be idle before it is disconnected. mode must be standalone. | 5 |
| interface <name> | Enter an interface name to associate the modem interface with the Ethernet interface that you want to either back up (backup configuration) or replace (standalone configuration). | No default. |
| mode <mode> | Enter the required mode: • standalone The modem interface is the connection from the FortiWiFi unit to the Internet. • redundant The modem interface automatically takes over from a selected Ethernet interface when that Ethernet interface is unavailable. | standalone |
| passwd1 <password_srt> | Enter the password used to access the specified dialup account. | No default |
| passwd2 <password_str> | Enter the password used to access the specified dialup account. | No default. |
| passwd3 <password_str> | Enter the password used to access the specified dialup account | No default. |

| | | |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| peer_modem1 {actiontec ascendTNT generic} | If the modem at phone1 is Actiontec or AscendTNT, select that type, otherwise leave setting as generic. This setting applies to the FortiWiFi-60AM only. | generic |
| peer_modem2 {actiontec ascendTNT generic} | If the modem at phone2 is Actiontec or AscendTNT, select that type, otherwise leave setting as generic. This setting applies to the FortiWiFi-60AM only. | generic |
| peer_modem3 {actiontec ascendTNT generic} | If the modem at phone3 is Actiontec or AscendTNT, select that type, otherwise leave setting as generic. This setting applies to the FortiWiFi-60AM only. | generic |
| phone1 <phone-number> | Enter the phone number required to connect to the dialup account. Do not add spaces to the phone number. Make sure to include standard special characters for pauses, country codes, and other functions as required by your modem to connect to your dialup account | No default. |
| phone2 <phone-number> | Enter the phone number required to connect to the dialup account. Do not add spaces to the phone number. Make sure to include standard special characters for pauses, country codes, and other functions as required by your modem to connect to your dialup account. | No default. |
| phone3 <phone-number> | Enter the phone number required to connect to the dialup account. Do not add spaces to the phone number. Make sure to include standard special characters for pauses, country codes, and other functions as required by your modem to connect to your dialup account. | No default. |
| redial <tries_interger> | Set the maximum number of times (1-10) the FortiWiFi unit dials the ISP to restore an active connection on the modem interface. Select <i>none</i> to allow the modem to redial without a limit. | No default. |
| status {disable enable} | Enable or disable modem support. | disable |
| username1 <name_str> | Enter the user name used to access the specified dialup account | No default. |
| username2 <name_str> | Enter the user name used to access the specified dialup account. | No default. |
| username3 <name_str> | Enter the user name used to access the specified dialup account. | No default. |

Example

```

config system modem
    set action dial
    set status enable
    set holddown-time 5
    set interface wan1
    set passwd1 acctlpasswd
    set phone1 1235551001
    set redial 10
    set username1 acctluser
end

```

Adding a Ping Server

Adding a ping server is required for routing failover for the modem in redundant mode. A ping server confirms the connectivity to an Ethernet interface.

To add a ping server to an interface

- 1 Go to **System > Network > Interface**.
- 2 Choose an interface and select Edit.
- 3 Set Ping Server to the IP address of the next hop router on the network connected to the interface.
- 4 Select the Enable check box.
- 5 Select OK to save the changes.

Dead gateway detection

The FortiWiFi unit uses dead gateway detection to ping the Ping Server IP address to make sure the FortiWiFi unit can connect to this IP address.

Modify dead gateway detection to control how the FortiWiFi unit confirms connectivity with a ping server added to an interface configuration. For information about adding a ping server to an interface, see above.

To modify the dead gateway detection settings

- 1 Go to **System > Network > Options**.
- 2 For Detection Interval, type a number in seconds to specify how often the FortiWiFi unit tests the connection to the ping target.
- 3 For Fail-over Detection, type a number of times that the connection test fails before the FortiWiFi unit assumes the gateway is no longer functioning.
- 4 Select Apply.

Adding firewall policies for modem connections

The modem interface requires firewall addresses and policies. You can add one or more addresses to the modem interface. For information about adding addresses, see the [FortiGate Administration Guide](#). When you add addresses, the modem interface appears on the policy grid.

You can configure firewall policies to control the flow of packets between the modem interface and the other interfaces on the FortiWiFi unit. For information about adding firewall policies, see the [FortiGate Administration Guide](#).

Using a wireless network

In a wired network, computers are connected through a series of cables that transfer information. In a wireless network, information is transferred over radio waves. There are factors which affect the transmission of data “on the air” that you must take into account when setting up a wireless network.

This section outlines the considerations for wireless networking and steps you can take to make your wireless network as efficient as possible.

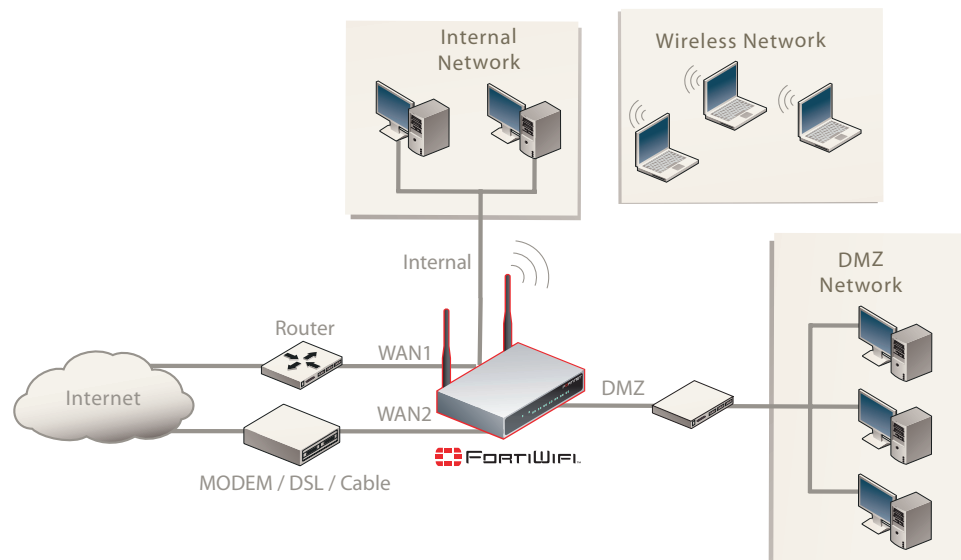
This section includes the following topics:

- [Setting up a wireless network](#)
- [Wireless Security](#)
- [FortiWiFi operation modes](#)
- [Setting up the FortiWiFi unit as an Access Point](#)

Setting up a wireless network

In its simplest form, a wireless network is an Access Point communicating with one wireless device. An Access Point (AP) is a device that provides a communications hub for a wireless network. The AP and the wireless devices operate on a common radio channel. The FortiWiFi unit acts as an AP and assigns all wireless users to the same subnet. With the proper firewall policies and routing, wireless users can communicate with users on the internal network or on an external network such as the Internet.

Figure 10: FortiWiFi unit as an Access Point



Positioning an Access Point

When placing the FortiWiFi AP, your main concern is providing a strong signal to all users. A strong signal ensures a fast connection and the efficient transfer of data. A weaker signal means a greater chance of data transmission errors and the need to re-send information, slowing down data transfer.

Consider the following guidelines when placing the FortiWiFi AP:

- Physical barriers can impede the radio signals. Solid objects such as walls, furniture and people absorb radio waves, weakening the signal. Be aware of the physical barriers in your office space that may reduce a signal. If there is enough physical interference, you may encounter dead spots that receive no signals.
- Ensure the FortiWiFi AP is located in a prominent location within a room for maximum coverage, rather than in a corner.
- Construction materials used in a building can also weaken radio signals. Rooms with walls of concrete or metal can affect the signal strength.

Radio Frequency interface

The 802.11b/g standard uses a frequency range of 2.4 to 2.483 GHz and the 802.11a standard transmit at 5 GHz. Radio frequency (RF) interference occurs when other devices send RF signals during their normal operation that use the same frequency as the FortiWiFi AP. Wireless devices such as cordless phones, microwave ovens and Bluetooth devices can interfere with packet transmissions on a wireless network.

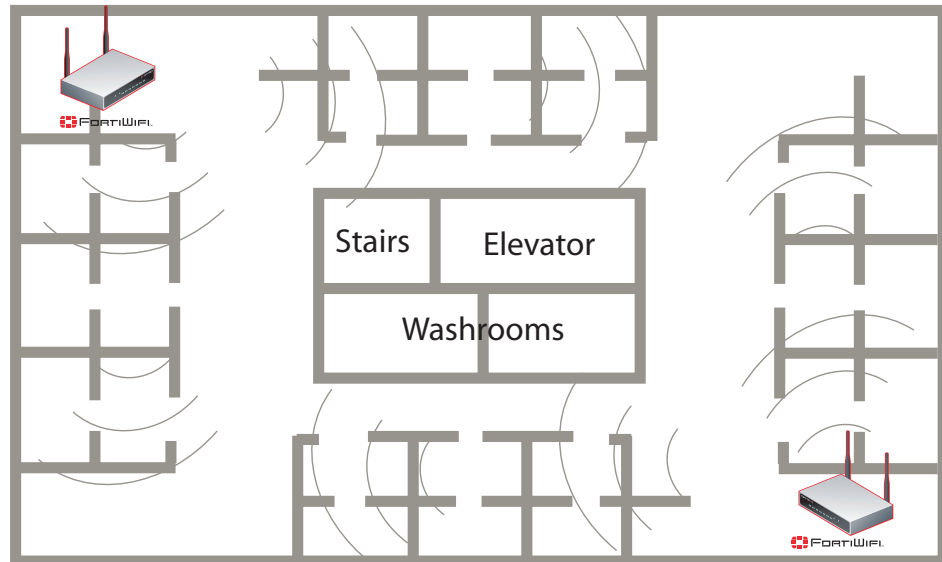
To avoid RF interference:

- Remove these devices from the immediate area where users are working. Something as simple as a Bluetooth enabled mouse may cause transmission interruptions.
- Keep the FortiWiFi AP and wireless devices at least 10 feet away from appliances such as microwave ovens and cordless phones.
- If you must have a cordless phone, select one that does not use the 2.4GHz frequency range for b/g or 5GHz frequency range for wireless a.
- Consider more FortiWiFi APs to help strengthen the signal. The weaker the signal, the slower the transmission will be as it tries to compete against other wireless devices.
- Set a channel that users and FortiWiFi APs will specifically use can improve signal quality.

Using multiple access points

If you cannot avoid some of these impediments due to the shape of the office or building materials used, you may need to use multiple FortiWiFi APs to help distribute the radio signal around the room. [Figure 11](#) shows how positioning two FortiWiFi APs within a uniquely shaped office space helps to distribute signals around the area.

Figure 11: Using multiple APs to provide a constant strong signal.



This sample office has washrooms, a stairwell and an elevator shaft in the center of the building, making it impossible to use a single FortiWiFi AP effectively. The elevator shaft and multiple metal stalls in the washrooms can cause signal degradation. However, placing a FortiWiFi AP in opposite corners of the office provides maximum coverage.

When using multiple APs, each FortiWiFi AP should be set to a different channel to avoid interference in areas where signals from both FortiWiFi units can be received.

Wireless Security

Radio waves transmitted between a wireless device and access points provide the weakest link between the wireless device and network servers. Wireless networking can be risky because information travels on radio waves, which is a public medium. The 802.11 standard includes security options to stop your information from being intercepted by unwanted sources. These are Wireless Equivalent Privacy (WEP) and WiFi Protected Access (WPA) encryption. Wireless encryption is only used between the wireless device and the AP. The AP decrypts the data before sending it along the wired network. The FortiWiFi unit supports both encryption methods.

Wireless Equivalent Privacy (WEP)

WEP security uses an encryption key between the wireless device and the AP. For WEP security, the wireless device and AP must use the same encryption key, and is manually typed by the wireless user and administrator. When activated, the wireless device encrypts the data with the encryption key for each frame using RSA RC4 ciphers.

There has been criticism of WEP security. WEP keys are static. They must be changed manually and frequently on both the wireless device and the APs. On a small company or network with a few users and APs, this is not a big issue. However, the more users and APs, changing WEP keys regularly can become an administrative headache and potentially error prone. Consequently, keys are rarely changed over months or years, leaving a hacker plenty of time to get the key and gain access to the network.

In small wireless networking environments, activating WEP security will significantly minimize outside infiltrators from getting in your network and is better than no security at all. However, it is still very important that you regularly change the WEP key, at least weekly; or monthly at most.

Wi-Fi Protected Access (WPA)

WPA was developed to replace the WEP standard and provide a higher level of data protection for wireless networks. WPA provides two methods of authentication; through 802.1X authentication or pre-shared keys.

802.1X authenticates users through an EAP authentication server such as a RADIUS server authenticates each user before they can connect to the network. The encryption keys can be changed at varying intervals to minimize the opportunity for hackers to crack the key being used.

In a network setup where a RADIUS server is not a viable option, WPA also provides authentication with preshared keys using Temporal Key Integrity Protocol (TKIP). Using TKIP, the encryption key is continuously re-keyed while the user is connected to the wireless network. This creates a unique key on every data packet. To further ensure data integrity, a Message Integrity Code (MIC also known as Michael) is incorporated into each packet. It uses an 8 byte message integrity code that is encrypted using the MAC addresses and data from each frame to provide a more secure packet transmission.

WPA provides a more robust security between the wireless device and the access point. The FortiWiFi unit supports both WPA methods.

Additional security measures

The FortiWiFi unit includes other security measures you can use to block unwanted users from accessing your wireless network. By setting a few extra options, you can be assured your network and its information is secure.

MAC address filtering

To improve the security of your wireless network, consider enabling MAC address filtering on the FortiWiFi unit. By enabling this feature, you define the wireless devices that can access the network based on their system MAC address. When a user attempts to access the wireless network, the FortiWiFi unit checks the MAC address of the user to the list you created. If the MAC address is on the approved list, the user gains access to the network. If the user is not in the list, the user is rejected. Using MAC address filtering makes it more difficult for a hacker using random MAC addresses or spoofing a MAC address to gain access to your network.

Service Set Identifier

The Service Set Identifier (SSID) is the network name shared by all users on a wireless network. Wireless users should configure their computers to connect to the network that broadcasts this network name. For security reasons, do not leave the default name of “fortinet” as the network name.

Broadcasting enables wireless users to find a network. The FortiWiFi unit includes an option not to broadcast the SSID. This provides an extra layer of protection. If you configure all wireless users to the correct SSID, you do not need to enable the broadcasting of the SSID.

To disable SSID

- 1 Go to **System > Wireless > Settings**.
- 2 Select the WLAN interface.
- 3 Clear SSID Broadcast.
- 4 Select OK.

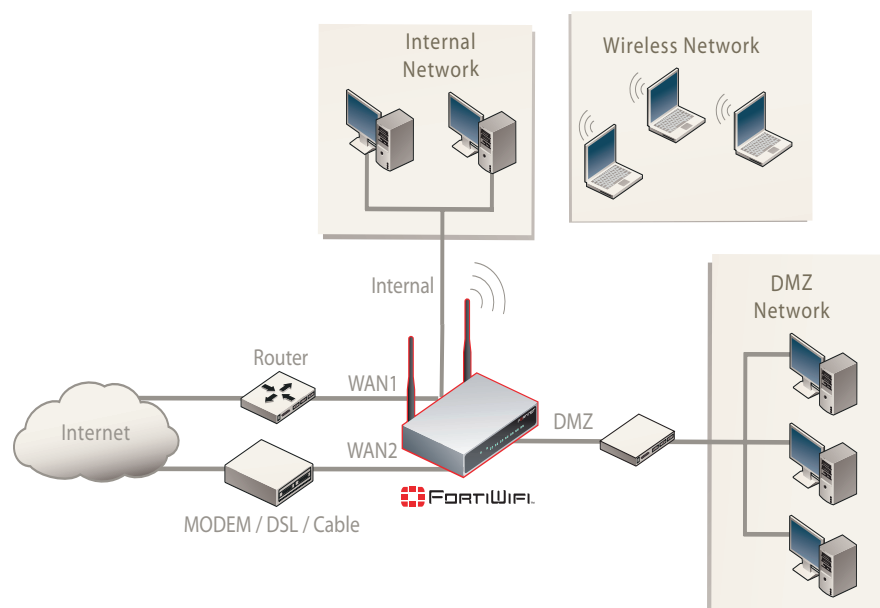
FortiWiFi operation modes

The FortiWiFi units have two modes of operation for wireless networking: Access Point and Client.

Access Point mode

When using the FortiWiFi unit in Access Point mode, the device acts as an access point for wireless users to connect to, send and receive information over a wireless network. It enables multiple wireless network users access to the network without the need to connect to it physically. The FortiWiFi unit can connect to the internal network and act as a firewall to the Internet. Access Point mode is the default mode.

Figure 12: FortiWiFi unit in Access Point mode

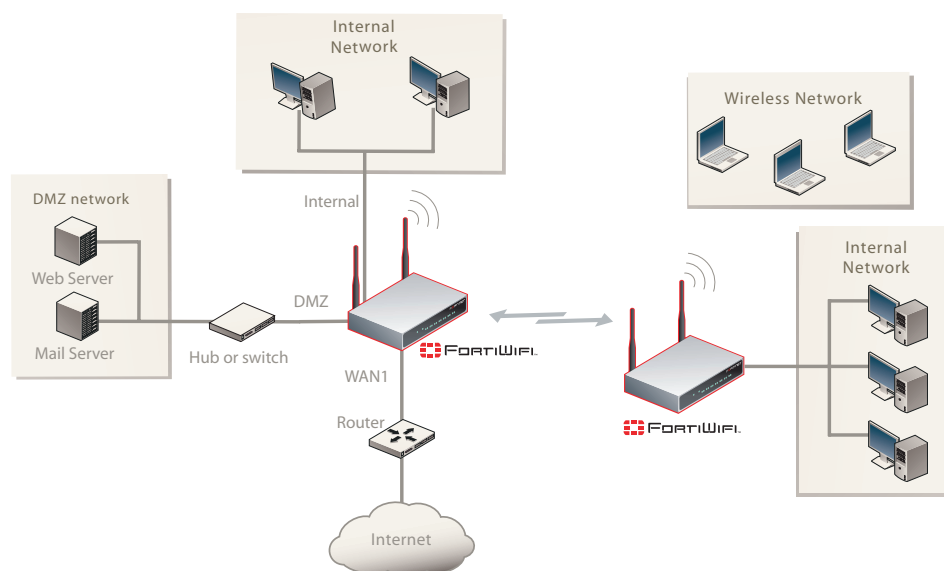


Client mode

When using the FortiWiFi unit in Client mode, the device is set to receive transmissions from another access point. This enables you to connect remote users to an existing network using wireless protocols from a location that does not have a wired infrastructure.

For example, in a warehouse where shipping and receiving are on opposite sides of the building, running cables is not an option due to the warehouse environment. The FortiWiFi unit can support wired users using its 4 Ethernet ports and can connect to another Access Point wirelessly as a Client. This connects the wired users to the network using the 802.11 wireless standard as a backbone.

Figure 13: FortiWiFi unit in Client mode



Changing the operating mode

To change the wireless operating mode

- 1 Go to **System > Wireless > Settings**.
- 2 For the Operation mode, select Change
- 3 Select the desired operation mode and select Apply.

Setting up the FortiWiFi unit as an Access Point

This section describes how to quickly configure the FortiWiFi unit as an AP to allow network access for wireless workstations located on the same wireless LAN as the unit. It also describes how to configure firewall policies and wireless security features to provide a secure wireless environment. For initial setup, use a desktop computer on the internal network with TCP/IP set as a DHCP client

This section contains the following steps:

- [Set the DHCP settings](#)
- [Set the security options](#)
- [Configure the firewall policies](#)

Set the DHCP settings

Configure a DHCP server for the FortiWiFi WLAN interface. As a DHCP server, the interface dynamically assigns IP addresses to hosts on the network connected to the WLAN interface.

To configure the FortiWiFi unit to be a DHCP server

- 1 Go to **System > DHCP > Service**.
- 2 Select the blue triangle to expand the WLAN options.
- 3 Configure the DHCP server settings:

| | |
|----------------------|---------------------------------------------------------------------------------------------------------------------------|
| Name: | Enter a name of the DHCP sever. For example, DHCPSever_1. |
| Enable: | Select to enable the DHCP Server. |
| Type: | Select regular unless you are configuring for remote clients who will have an IPSec VPN connection to the WLAN interface. |
| IP Range: | Enter the IP address of the WLAN to configure the IP address range. For example, 10.10.80.1 to 10.10.80.20. |
| Network Mask: | Enter the network mask you created in Table 9 on page 33 . |
| Domain: | Enter domain name, for example, www.fortinet.com. |
| Lease Time: | The expiry date of an IP address. This feature specifies either an unlimited or limited timeframe of an IP address. |
| Advanced: | Use only to specify several DNS servers (including WIN servers) for the interface. |
- 4 Select OK.



Note: The IP range must match the subnet address of the network where the DHCP request was received. Usually this would be the subnet connected to the WLAN interface.

Set the security options

To ensure proper security and protection of your network and its information, set the security options for the FortiWiFi unit.

To set the data security

- 1 Go to **System > Wireless > Settings**.
- 2 Select the WLAN interface.
- 3 Enter an SSID.
- 4 Set the SSID Broadcast to either enable or disable.
- 5 Select a Security mode.
- 6 Enter a key or pre-shared key depending on the Security Mode selected.
- 7 Select the MAC Filter tab.
- 8 Enable MAC filtering if desired and select Edit.

- 9 Enter the MAC addresses and select to Allow or Deny them from the wireless network.



Note: You will need to distribute the information entered in step 2 and step 5 with the wireless users so they can connect to the wireless network.



Note: It is highly recommended you do not select "None". Selecting None will leave your wireless network prone to hackers.

Configure the firewall policies

The FortiWiFi unit provides WAN interfaces for Internet connections. You can configure the Internet connection for both wired networks on the internal and/or DMZ interfaces and the wireless network through the WLAN interface.

You can provide secure Internet access for wireless clients by creating firewall policies from the WLAN interface to the WAN1 or WAN2 interfaces.

The following example creates a policy from the wireless clients (WLAN interface) to the Internet (WAN1 interface) using traffic shaping, firewall authentication and the default Strict content policy.

To create a new wall policy for a secure Internet connection

- 1 Go to **Firewall > Policy**.
- 2 Select the blue arrow for WLAN to WAN1.
- 3 Select Create New.

Configure the following settings:

| | |
|-----------------------------------|--------|
| Interface/Zone Source | WLAN |
| Interface/Zone Destination | WAN1 |
| Address Name Source | All |
| Address Name Destination | All |
| Schedule | Always |
| Service | ANY |
| Action | ACCEPT |
| NAT | Enable |
| Protection Profile | Strict |

- 4 Select Advanced.
- 5 Select Traffic Shaping.
- 6 Configure traffic shaping bandwidth and Traffic Priority settings to meet your requirements.
- 7 Select OK.

FortiWiFi Firmware

Fortinet periodically updates the FortiWiFi firmware to include enhancements and address issues. After you have registered your FortiWiFi unit, FortiWiFi firmware is available for download at <http://support.fortinet.com>.

Only the FortiWiFi administrators (whose access profiles contain system configuration read and write privileges) and the FortiWiFi admin user can change the FortiWiFi firmware.

This section includes the following topics:

- [Upgrading to a new firmware version](#)
- [Reverting to a previous firmware version](#)
- [Installing firmware images from a system reboot using the CLI](#)
- [The FortiUSB key](#)
- [Testing a new firmware image before installing it](#)



Note: If you have an earlier version of the FortiOS firmware, for example FortiOS v2.50, upgrade to FortiOS v2.80MR10 (or FortiOS v2.80MR11) before upgrading to FortiOS v3.0.

Upgrading to a new firmware version

Use the web-based manager or CLI procedure to upgrade to a new FortiOS firmware version or to a more recent build of the same firmware version.

Upgrading the firmware using the web-based manager

Use the following procedures to upgrade the FortiWiFi unit to a new firmware version.



Note: Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. For details see the [FortiGate Administration Guide](#).



Note: To use this procedure, you must log in using the admin administrator account, or an administrator account that has system configuration read and write privileges.

To upgrade the firmware using the web-based manager

- 1 Copy the firmware image file to your management computer.
- 2 Log into the web-based manager as the admin administrative user.
- 3 Go to **System > Status**.
- 4 Under **System Information > Firmware Version**, select Update.
- 5 Type the path and filename of the firmware image file, or select Browse and locate the file.

- 6 Select OK.
The FortiWiFi unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiWiFi login. This process takes a few minutes.
- 7 Log into the web-based manager.
- 8 Go to **System > Status** and check the firmware version to confirm the firmware upgrade is successfully installed.
- 9 Update antivirus and attack definitions. For information about updating antivirus and attack definitions, see the [FortiGate Administration Guide](#).

Upgrading the firmware using the CLI

To use the following procedure, you must have a TFTP server the FortiWiFi unit can connect to.



Note: Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute update-now` to update the antivirus and attack definitions. For details, see the [FortiGate Administration Guide](#).



Note: To use this procedure, you must log in using the admin administrator account, or an administrator account that has system configuration read and write privileges.

To upgrade the firmware using the CLI

- 1 Make sure the TFTP server is running.
- 2 Copy the new firmware image file to the root directory of the TFTP server.
- 3 Log into the CLI.
- 4 Make sure the FortiWiFi unit can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiWiFi unit:

```
execute restore image TFTP <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image image.out 192.168.1.168
```

The FortiWiFi unit responds with the message:

```
This operation will replace the current firmware version!  
Do you want to continue? (y/n)
```

- 6 Type `y`.
The FortiWiFi unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.
- 7 Reconnect to the CLI.

- 8 To confirm the new firmware image is successfully installed, enter:

```
get system status
```
- 9 Update antivirus and attack definitions (see the [FortiGate Administration Guide](#)), or from the CLI, enter:

```
execute update-now
```

Reverting to a previous firmware version

Use the following procedures to revert your FortiWiFi unit to a previous firmware version.

Use the web-based manager or CLI procedure to revert to a previous firmware version. This procedure reverts the FortiWiFi unit to its factory default configuration.

Reverting to a previous firmware version using the web-based manager

The following procedures revert the FortiWiFi unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure, it is recommended that you:

- back up the FortiWiFi unit configuration
- back up the IPS custom signatures
- back up web content and email filtering lists

For more information, see the [FortiGate Administration Guide](#).

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v3.0 to FortiOS v2.80), you might not be able to restore the previous configuration from the backup configuration file.



Note: Installing firmware replaces the current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. For details, see the [FortiGate Administration Guide](#). You can also use the CLI command `execute update-now` to update the antivirus and attack definitions.



Note: To use this procedure, you must log in using the admin administrator account, or an administrator account that has system configuration read and write privileges.

To revert to a previous firmware version using the web-based manager

- 1 Copy the firmware image file to the management computer.
- 2 Log into the FortiWiFi web-based manager.
- 3 Go to **System > Status**.
- 4 Under **System Information > Firmware Version**, select Update.
- 5 Type the path and filename of the firmware image file, or select Browse and locate the file.

6 Select OK.

The FortiWiFi unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiWiFi login. This process takes a few minutes.

7 Log into the web-based manager.**8** Go to **System > Status** and check the Firmware Version to confirm the firmware is successfully installed.**9** Restore your configuration.

For information about restoring your configuration, see the [FortiGate Administration Guide](#).

10 Update antivirus and attack definitions.

For information about antivirus and attack definitions, see the [FortiGate Administration Guide](#).

Reverting to a previous firmware version using the CLI

This procedure reverts the FortiWiFi unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to the replacement messages.

Before beginning this procedure, it is recommended that you:

- back up the FortiWiFi unit system configuration using the command `execute backup config`
- back up the IPS custom signatures using the command `execute backup ipsuserdefsig`
- back up web content and email filtering lists

For more information, see the [FortiGate Administration Guide](#).

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v3.0 to FortiOS v2.80), you might not be able to restore your previous configuration from the backup configuration file.



Note: Installing firmware replaces the current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. For details, see the [FortiGate Administration Guide](#). You can also use the CLI command `execute update_now` to update the antivirus and attack definitions.



Note: To use this procedure, you must log in using the admin administrator account, or an administrator account that has system configuration read and write privileges.

To use the following procedure, you must have a TFTP server the FortiWiFi unit can connect to.

To revert to a previous firmware version using the CLI

- 1** Make sure the TFTP server is running.
- 2** Copy the firmware image file to the root directory of the TFTP server.
- 3** Log into the FortiWiFi CLI.

- 4 Make sure the FortiWiFi unit can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiWiFi unit:

```
execute restore image TFTP <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image TFTP image.out
```

```
192.168.1.168
```

The FortiWiFi unit responds with the message:

```
This operation will replace the current firmware version!  
Do you want to continue? (y/n)
```

- 6 Type `y`.

The FortiWiFi unit uploads the firmware image file. After the file uploads, a message similar to the following is displayed:

```
Get image from tftp server OK.
```

```
Check image OK.
```

```
This operation will downgrade the current firmware version!  
Do you want to continue? (y/n)
```

- 7 Type `y`.

The FortiWiFi unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.

- 8 Reconnect to the CLI.

- 9 To confirm the new firmware image has been loaded, enter:

```
get system status
```

- 10 To restore your previous configuration, if needed, use the command:

```
execute restore config TFTP <name_str> <tftp_ipv4>
```

- 11 Update antivirus and attack definitions.

For information, see the [FortiGate Administration Guide](#), or from the CLI, enter:

```
execute update-now
```

Installing firmware images from a system reboot using the CLI

This procedure installs a specified firmware image and resets the FortiWiFi unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware version.

Use this procedure to install a new firmware version or revert to a previous firmware version. To use this procedure, you must connect to the CLI using the FortiWiFi console port and a RJ-45 to DB-9 serial cable. This procedure reverts the FortiWiFi unit to its factory default configuration.



Note: This procedure varies for different FortiWiFi BIOS versions. These variations are explained in the procedure steps that are affected. The version of the BIOS running on the FortiWiFi unit is displayed when you restart the FortiWiFi unit using the CLI through a console connection.

For this procedure you:

- Access the CLI by connecting to the FortiWiFi console port using a RJ-45 to DB-9 serial cable.
- Install a TFTP server that you can connect to from the FortiWiFi internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, it is recommended that you:

- back up the FortiWiFi unit configuration
- back up the IPS custom signatures
- back up web content and email filtering lists

For more information, see the [FortiGate Administration Guide](#).

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v3.0 to FortiOS v2.80), you might not be able to restore your previous configuration from the backup configuration file.



Note: Installing firmware replaces the current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. For information, see the [FortiGate Administration Guide](#).

To install firmware from a system reboot

- 1 Connect to the CLI using the RJ-45 to DB-9 cable/console port.
- 2 Make sure the TFTP server is running.
- 3 Copy the new firmware image file to the root directory of the TFTP server.
- 4 Make sure the internal interface is connected to the same network as the TFTP server.
- 5 To confirm the FortiWiFi unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168, enter:

```
execute ping 192.168.1.168
```

- 6 Enter the following command to restart the FortiWiFi unit:

```
execute reboot
```

The FortiWiFi unit responds with the following message:

```
This operation will reboot the system !
Do you want to continue? (y/n)
```

- 7 Type `y`.

As the FortiWiFi unit starts, a series of system startup messages is displayed.

When one of the following messages appears:

- FortiWiFi unit running v2.x BIOS
Press Any Key To Download Boot Image.
...
- FortiWiFi unit running v3.x BIOS
Press any key to display configuration menu.....

Immediately press any key to interrupt the system startup.



Note: You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiWiFi unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, one of the following messages appears:

- FortiWiFi unit running v2.x BIOS
Enter TFTP Server Address [192.168.1.168]:
Go to step 9.
- FortiWiFi unit running v3.x BIOS
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

```
Enter G,F,Q, or H:
```

- 8 Type `G` to get the new firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

- 9 Type the address of the TFTP server and press `Enter`.

The following message appears:

```
Enter Local Address [192.168.1.188]:
```

- 10 Type an IP address that can be used by the FortiWiFi unit to connect to the FTP server.

The IP address can be any IP address that is valid for the network the interface is connected to. Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

- 11 Enter the firmware image filename and press Enter.

The TFTP server uploads the firmware image file to the FortiWiFi unit and messages similar to the following are displayed:

- FortiWiFi unit running v2.x BIOS
Do You Want To Save The Image? [y/n]
Type y.
- FortiWiFi unit running v3.x BIOS
Save as Default firmware/Run image without saving:[D/R]

- 12 Type D.

The FortiWiFi unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

Restoring the previous configuration

Change the internal interface address, if required. You can do this from the CLI using the following command:

```
config system interface
  edit internal
    set ip <address_ipv4mask>
    set allowaccess {ping https ssh telnet http}
  end
```

After changing the interface address, you can access the FortiWiFi unit from the web-based manager and restore the configuration.

For more information, see the [FortiGate Administration Guide](#).

If you are reverting to a previous firmware version (for example, reverting from FortiOS v3.0 to FortiOS v2.80), you might not be able to restore your previous configuration from the backup up configuration file.

The FortiUSB key

The FortiUSB key provides flexibility and control when backing up and restoring configuration files. The FortiUSB key also enables you to have a single, secure location for storing configuration files.

The FortiUSB key is used with the USB Auto-Install feature, automatically installing a configuration file and a firmware image file on a system reboot. The USB Auto-Install feature uses a configuration file and a firmware image file that is on the FortiUSB key, and on a system reboot, checks if these files need to be installed. If they do, the FortiWiFi unit installs the configuration file and firmware image file directly from the key to the unit.



Note: The FortiUSB key is purchased separately. The FortiWiFi unit only supports the FortiUSB key available from Fortinet.

Backup and Restore from the FortiUSB key

You can use the FortiUSB key to either backup a configuration file or restore a configuration file.

You should always make sure the FortiUSB key is properly install before proceeding since the FortiWiFi unit must recognize that the key is installed in its USB port. The FortiUSB key may not be recognized by the FortiWiFi unit if it is inserted when the unit is running. If the key is unrecognized by the FortiWiFi unit, you will be unable to properly backup your configuration.



Note: You can only save VPN certificates if you encrypt the file. Make sure the configuration encryption is enabled so you can save the VPN certificates with the configuration file. However, an encrypted file is ineffective if selected for the USB Auto-Install feature.

To backup configuration using the web-based manager

- 1 Go to **System > Maintenance > Backup and Restore**.
- 2 Select USB Disk from the backup configuration to list.
- 3 Enter a filename for the configuration file.
- 4 Select Backup.

To restore configuration web-based manager

- 1 Go to **System > Maintenance > Backup and Restore**.
- 2 Select USB Disk from the restore configuration from list.
- 3 Select a backup configuration file from the list.
- 4 Select Restore.

To backup configuration using the CLI

- 1 Log into the CLI.
- 2 Enter the following command to backup the configuration files:
`exec backup config usb <filename>`
- 3 Enter the following command to check the configuration files are on the key:
`exec usb-disk list`

To restore configuration using the CLI

- 1 Log into the CLI.
- 2 Enter the following command to restore the configuration files:
`exec restore image usb <filename>`

The FortiWiFi unit responds with the following message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

- 3 Type `y`.

Using the USB Auto-Install feature

The USB Auto-Install feature automatically updates the FortiWiFi configuration file and image file on a system reboot. Also, this feature provides you with an additional backup if you are unable to save your system settings before shutting down or rebooting your FortiWiFi unit.

You need to do the following before configuring the USB Auto-Install feature:

- power off the FortiWiFi unit
- install the FortiUSB key
- power up the FortiWiFi unit

The following procedures use both the web-based manager and the CLI. However, it is recommended you use the CLI since the login screen may appear before the installation is complete. The FortiWiFi unit may reboot twice if installing the firmware image and configuration file.



Note: You need an unencrypted configuration file for this feature. Also the default files, image.out and fgt_system.conf, must be in the root directory.



Note: Make sure FortiOS v3.0MR1 is installed on the FortiWiFi unit before installing.

To configure the USB Auto-Install using the web-based manager

- 1 Go to **System > Maintenance > Backup and Restore**.
- 2 Select the blue arrow to expand the Advanced options.
- 3 Select the following:
 - On system restart, automatically update FortiWiFi configuration file if default filename is available on the USB disk.
 - On system restart, automatically update FortiWiFi firmware image if default image is available on the USB disk.
- 4 Enter the configuration and image filenames or use the default configuration filename (system.conf) and default image name (image.out).
- 5 The default configuration filename should show in the Default configuration file name field.
- 6 Select Apply.

To configure the USB Auto-Install using the CLI

- 1 Log into the CLI.
- 2 Enter the following command:


```
config system auto-install
    set default-config-file <filename>
    set auto-intall-config <enable/disable>
    set default-image-file <filename>
    set auto-install-image <enable/disable>

end
```
- 3 Enter the following command to see the new firmware installation settings:


```
get system status
```

Additional CLI Commands for the FortiUSB key

Use the following CLI commands when you want to delete a file from the FortiUSB key, list what files are on the key, including formatting the key or renaming a file:

- `exec usb-disk list`
- `exec usb-disk delete <filename>`
- `exec usb-disk format`
- `exec usb-disk rename <old_filename1> <old_filename2>`



Note: If you are trying to delete a configuration file from the CLI command interface, and the filename contains spaces, you will need quotations around the filename before you can delete the file from the FortiUSB key.

Testing a new firmware image before installing it

You can test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure, the FortiWiFi unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiWiFi unit restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure ["Upgrading to a new firmware version" on page 65](#).

Use this procedure to test a new firmware image before installing it. To use this procedure, you must connect to the CLI using the RJ-45 to DB-9 serial cable/console port. This procedure temporarily installs a new firmware image using your current configuration.

For this procedure you:

- Access the CLI by connecting to the FortiWiFi console port using a RJ-45 to DB-9 serial cable/console port.
- Install a TFTP server that you can connect to from the FortiWiFi internal interface. The TFTP server should be on the same subnet as the internal interface.

To test a new firmware image

- 1 Connect to the CLI using a RJ-45 to DB-9 serial cable/console port.
- 2 Make sure the TFTP server is running.
- 3 Copy the new firmware image file to the root directory of the TFTP server.
- 4 Make sure the internal interface is connected to the same network as the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to restart the FortiWiFi unit:

```
execute reboot
```

- 6** As the FortiWiFi unit reboots, press any key to interrupt the system startup. As the FortiWiFi unit starts, a series of system startup messages are displayed.

When one of the following messages appears:

- FortiWiFi unit running v2.x BIOS
Press Any Key To Download Boot Image.
...
- FortiWiFi unit running v3.x BIOS
Press any key to display configuration menu.....

- 7** Immediately press any key to interrupt the system startup.



Note: You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiWiFi unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, one of the following messages appears:

- FortiWiFi unit running v2.x BIOS
Enter TFTP Server Address [192.168.1.168]:
Go to step [9](#).
- FortiWiFi unit running v3.x BIOS
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G,F,Q, or H:

- 8** Type G to get the new firmware image from the TFTP server.

The following message appears:

Enter TFTP server address [192.168.1.168]:

- 9** Type the address of the TFTP server and press Enter.

The following message appears:

Enter Local Address [192.168.1.188]:

- 10** Type an IP address that can be used by the FortiWiFi unit to connect to the TFTP server.

The IP address can be any IP address that is valid for the network the interface is connected to. Make sure you do not enter the IP address of another device on this network.

The following message appears:

Enter File Name [image.out]:

- 11** Enter the firmware image file name and press Enter.
The TFTP server uploads the firmware image file to the FortiWiFi unit and messages similar to the following appear.
- FortiWiFi unit running v2.x BIOS
Do You Want To Save The Image? [Y/n]
Type n.
 - FortiWiFi unit running v3.x BIOS
Save as Default firmware/Run image without saving:[D/R]
- 12** Type R.
The FortiWiFi image is installed to system memory and the FortiWiFi unit starts running the new firmware image but with its current configuration.
- 13** You can log into the CLI or the web-based manager using any administrative account.
- 14** To confirm the new firmware image has been loaded, from the CLI enter:
`get system status`
You can test the new firmware image as required.

Index

Numerics

802.11 standard 58

A

access point 57
adding a default route 35, 37
auto-dial 52

C

certificate, security 18
CLI
 additional commands for FortiUSB key 75
 configuring NAT/Route mode 35
 connecting 19
 upgrading the firmware 66, 68
client mode 62
comments, documentation 13
configuring
 redundant mode 50
 standalone mode 50
connecting
 to the CLI 19
 to the web-based manager 18
customer service 13

D

dashboard, system 19
dead gateway detection 56
default
 gateway 24
 protection profiles 26
 restoring settings 27
DHCP
 configuration 33
 starting IP 24
 wireless 63
dial now button 52
dial on demand 52
documentation
 commenting on 13
 Fortinet 12

F

factory defaults
 DHCP server configuration 24
 firewall configuration 25
 NAT/Route mode config 24
 protection profiles 26
 Transparent mode config 25
firewall policies
 modem 56
 wireless 64
firmware
 backup and restore from FortiUSB key 73

installing 70
re-installing current version 70
restoring previous config 72
reverting to an older version 70
testing firmware image 75
upgrading to a new version 65
upgrading using the CLI 66, 68
upgrading using the web-base manager 65, 67

FortiGate documentation
 commenting on 13
Fortinet customer service 13
Fortinet documentation 12
Fortinet Family Products 8
 FortiBridge 9
 FortiClient 8
 FortiGuard 8
 FortiLog 9
 FortiMail 9
 FortiManager 9
 FortiReporter 9
Fortinet Knowledge Center 13
FortiUSB key
 additional CLI commands 75
 backup and restore 73
 USB Auto-Install 74
frequency 58

H

hang up button 52
holddown timer 52

I

idle timeout 52
installing factory defaults 20
interference 58
introduction
 Fortinet documentation 12

L

lease duration
 DHCP 24
LED descriptions 16

M

MAC address filtering 60
Message Integrity Code (MIC) 60
modem
 adding firewall policies 56
 configuring settings 51
 mode 52
 redundant mode 49
 standalone mode 49, 50
 status 52
mounting 16

N

- NAT/Route mode
 - settings 33
 - using the CLI 35
 - using web-based manager 33
- network ID 61
- NTP server 43
 - synchronize 44

P

- ping server 56
- PPPoE configuration 33
- products, Fortinet family 8
- protection profiles, default 26

R

- reconnecting to the web-based manager 42
- redial limit 52
- redundant mode
 - configuring 50
 - modem 49
- registering the FortiGate unit 8
- restoring
 - previous config, firmware 72
- restoring default settings 27
- reverting, to an older firmware version 70
- RSA RC4 59

S

- security
 - MAC address filtering 60
 - WEP 59
 - wireless 59
 - WPA 60
- security certificate 18
- Service Set Identifier (SSID) 61
- set time 43
- standalone mode
 - configuring 50
 - modem 49, 50
- starting IP, DHCP 24

- synchronize with NTP server 44
- System dashboard 19

T

- technical support 13
- time zone 43
- TKIP 60
- Transparent mode
 - changing to 41
 - settings 40
 - using the CLI 41
 - using web-based manager 40

U

- updating
 - adding override server 46
 - antivirus and IPS, web-based manager 44
 - IPS using CLI 45
 - scheduling updates 45
- upgrading
 - firmware 65
 - firmware using the CLI 66, 68
 - firmware using the web-based manager 65, 67
- USB Auto-Install 74
- using web-based manager 40

V

- verifying
 - connection 38, 42
 - connection, web-based manager 35
 - web-based manager, config 35

W

- web-based manager, connecting 18
- Wi-Fi Protected Access (WPA) 60
- wireless
 - client mode 62
 - DHCP settings 63
 - firewall policies 64
 - network name 61
 - security 59
- Wireless Equivalent Privacy (WEP) 59

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com